Drug Enforcement Administration | Office of Diversion Control

E-Commerce Program

CSOS Certificate Support Guide

Version: 1.1
Published: October 1, 2006
Publisher: CSOS Certification Authority

Document Revision History

Version #	Revision Date	Sections Affected	Summary of Changes	Initials
1.0	4/27/2006	All	Version 1.0 published	TO
1.1	10/1/2006	Retrieval	Updated documentation to match new retrieval pages.	TO

Introduction

This Certificate Support Guide has been developed and is maintained by the Drug Enforcement Administration's CSOS Certification Authority. This Guide is intended to assist organizations implementing electronic controlled substance ordering. Specifically, the procedures in this guide should be used by chain pharmacy and wholesaler customer support when assisting CSOS Subscribers.

Organizations are not required to use this document, however variance from these documented procedures, especially those marked with an ⚠, may render certificates invalid and/or result in certificate revocation due to policy violations.

This Guide was developed using Windows XP Professional SP2, Microsoft Internet Explorer version 6.0, Netscape Browser 7.2 and 8.1, and Mozilla Firefox versions 1.0 and 1.5.

Comments, suggestions, and corrections are welcome and should be sent to DEA Diversion E-Commerce Support:

E-mail: CSOSsupport@DEAecom.gov
Phone: 877-332-3266

DEA Diversion E-Commerce Support is available to provide further explanation on issues discussed in this guide as well as any issues not covered.

Updates to this guide: DEA's CSOS Certification Authority will continue to update this Support Guide to ensure that the documentation provided is as thorough as possible. Feedback is welcome and appreciated. The most current version will be made available at the address below. Please check for periodic updates or E-mail CSOSsupport@DEAecom.gov to be notified when a new version of this Guide is released:

- http://www.deaecom.gov/wholesaler_support.html

Policy note: DEA's support staff will revoke subscriber certificates due to policy violations. Support representatives from wholesalers and chain pharmacies must be cognizant of proper certificate/private key handling procedures and should pay close attention to all notes in this document marked with the ⚠ icon.

Disclaimer: The procedures documented in this Certificate Support Guide are the DEA CSOS CA's recommendations for proper handling of CSOS Certificates. The policies discussed in this document abide by, but are not a replacement for, the Code of Federal Regulations, which governs electronic ordering of controlled substances. Please refer to www.DEAecom.gov/policies.html or contact DEA Diversion E-Commerce Support for all policy related questions.

Important Support Guidelines

Following the procedures of this Guide will help to ensure that customers are provided a high level of quality customer support. The following is a list of common policy violations and misperceptions addressed by this Guide.

- Never retrieve a certificate without the owner present.
- Each certificate may only be retrieved one time.
- Many CSOS subscribers are issued multiple certificates. While CSOS Administrative certificates are not used for ordering, they must be retrieved.
- The certificate's security level must always be set to high when using Internet Explorer.
- The certificate's password, entered during retrieval, is created by the certificate owner only and not provided by DEA. Do not use any DEA provided information, specifically the retrieval Access Code and Access Code Password, for the certificate's password.
- Only the owner of the certificate may set and have knowledge of the certificate's password. Neither DEA nor the certificate owner's co-workers, company, or wholesaler, may have knowledge of the certificate's password.
- CSOS Certificates are wholesaler independent, and therefore may be used to order from multiple wholesalers.
- CSOS Certificates may be installed on multiple computers.
- CSOS Certificates may be backed up onto CD or floppy disk, as long as each certificate is protected by a backup password and the media is securely stored (i.e. in a safe).
- Certificates should not be deleted from the browser's certificate store during export or after installation into the certificate store of the ordering software.
- Per Federal Regulations, please delete any unused PFX or P12 exported certificate files that have been installed into ordering software or a browser's certificate store.
- When exporting, backing up, and/or transferring certificates where a name must be given to the PFX or P12 certificate file, please use a meaningful naming convention as discussed in the Export and Backup sections of this Guide.
- Please contact DEA E-Commerce Support when unsure of a procedure or when having difficulty with any CSOS Certificate.
- When contacting DEA E-Commerce Support, please be ready to provide the customer's DEA Number(s), and if possible the customer's name and certificate serial number(s).

Table of Contents

1. Certification Authority (CA) Certificates 1

Introduction to the DEA E-Commerce Root CA Certificate 1
What is the Root CA certificate? 1
What is the Root CA used for? 1
How does the Root CA impact certificate support? 1

Introduction to the CSOS Sub CA Certificate 1
What is the CSOS Sub CA certificate? 1
What is the CSOS Sub CA certificate used for? 1
How does the CSOS Sub CA certificate impact certificate support? 1

CA Certificate Management 2
Internet Explorer 2
Root CA Certificate – Where is it published? 2
Root CA Certificate – Installation 2
Root CA Certificate – Install Verification 5
CSOS Sub CA Certificate – Where is it published? 6
CSOS Sub CA Certificate – Installation 6
CSOS Sub CA Certificate – Install Verification 9
Netscape 10
Root CA Certificate – Where is it published? 10
Root CA Certificate – Installation 10
Root CA Certificate – Install Verification 11
CSOS Sub CA Certificate – Where is it published? 11
CSOS Sub CA Certificate – Installation 11
CSOS Sub CA Certificate – Install Verification 12

2. Subscriber Certificate Retrieval 13

What information is needed for certificate retrieval? 14
Access Codes (Via E-mail) 14
Access Code Passwords (Via Postal Mail) 14
System and Browser Requirements 15

Certificate Retrieval Instructions 17
Subscriber Certificate Retrieval – Internet Explorer 17
Where is the certificate installed? 25
Subscriber Certificate Retrieval – Netscape 26
Where is the certificate installed? 33
Certificate Retrieval Error Codes 34
Error –1666 34
Error 2278 35
Error 2731 35
Error 3274 36
Error 3290 36
Error 8010001D or 8010002E 37

No key pair has been generated (no error number) ... 37
No providers are listed in the CSP dropdown list ... 38

3. Certificate Management ... 39

Where are certificates installed? ... 39

Finding certificates ... 39
Locating certificates in Internet Explorer ... 39
Locating certificates in Netscape 7.2 ... 40
Locating certificates in Netscape 8.1 ... 42
Locating certificates in Mozilla Firefox 1.5 ... 44
Locating certificates in Mozilla Firefox 1.0 ... 46
What to do if the certificate is not found in a browser ... 48
Locating certificates in the Microsoft Management Console (MMC) ... 49
Locating certificate files ... 54
Search using Windows XP: ... 54
Search using Windows 2000: ... 54

Identifying CSOS Certificates ... 55
Identify certificates using the expiration date (easiest method) ... 56
Identify using the Certificate Serial Number (more accurate method) ... 56
Identify certificates using valid ordering schedules (last resort method) ... 59

Certificate Export ... 60
Introduction on Certificate Export ... 60
Certificate Export - Internet Explorer ... 61
Certificate Export – Netscape ... 70
Certificate Export – Mozilla Firefox ... 73

Certificate Import ... 76
Certificate Import – Internet Explorer ... 76

Certificate Transfer ... 83

Private Key Password Reset ... 84

4. Terminology ... 86

5. DEA Diversion E-Commerce Support ... 89

1. Certification Authority (CA) Certificates

The **DEA E-Commerce Root CA** and **CSOS Sub CA** certificates must be installed on any computer used for electronic ordering of controlled substances. These CA certificates are found on the DEA E-Commerce Web site and may be installed at any time, on any computer system, by anyone.

Introduction to the DEA E-Commerce Root CA Certificate

What is the Root CA certificate?
The DEA E-Commerce Root CA Certificate is a self-signed certificate, meaning it was created by itself and must be explicitly trusted by each CSOS subscriber and relying party. Subscribers and relying parties must trust the Root CA in order to begin the trust relationship that is fundamental to the E-Commerce PKI system. To create the trust relationship, the Root CA Certificate must be installed in order to give validity to the CSOS Sub CA and any CSOS subscriber certificate(s).

What is the Root CA used for?

- Signing the CSOS Sub CA certificate
- Signing the Authority Revocation List (i.e. where revoked sub-CA certificates would be published)

How does the Root CA impact certificate support?
CSOS certificates will not be recognized as valid and trusted if the Root CA Certificate is not installed on the same system as the subscriber's certificate. For relying parties, the digital signature on the Authority Revocation List (ARL) cannot be authenticated unless the Root CA Certificate is installed on the same system where validation occurs.

Introduction to the CSOS Sub CA Certificate

What is the CSOS Sub CA certificate?
The CSOS Sub CA certificate is the certificate representing DEA's CSOS Subordinate CA that issues CSOS subscriber certificates. The Sub CA is issued by DEA's E-Commerce Root CA and inherits its trust from the Root CA. A Sub CA certificate is valid for six years, but is used for signing CSOS Subscriber certificates for a three (3) year period before a new Sub CA is issued by DEA.

What is the CSOS Sub CA certificate used for?

- Signing all CSOS subscriber certificates
- Signing the Certificate Revocation List (i.e. where revoked subscriber certificates are published)

How does the CSOS Sub CA certificate impact certificate support?
CSOS certificates will not be recognized as valid and trusted if the CSOS Sub CA certificate is not installed on the same system as the subscriber's certificate. Supplier systems will not be able

to verify the validity of the purchaser's CSOS Certificate if the certificate's issuing Sub CA certificate is not installed on the validation system.

CA Certificate Management

Internet Explorer

The following instructions are specific to Microsoft Internet Explorer version 6.0. Instructions for the Netscape Browser are available in the following section.

Root CA Certificate – Where is it published?

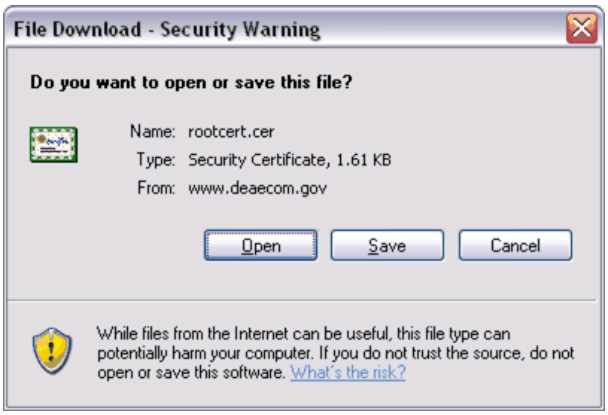
The Root CA certificate may be found on the DEA E-Commerce Web site in one of two locations:

- In the Certificate Management section of the site
  - www.deaecom.gov/certmanage.html
- In the Certificate Retrieval section of the site
  - Private link provided to subscribers

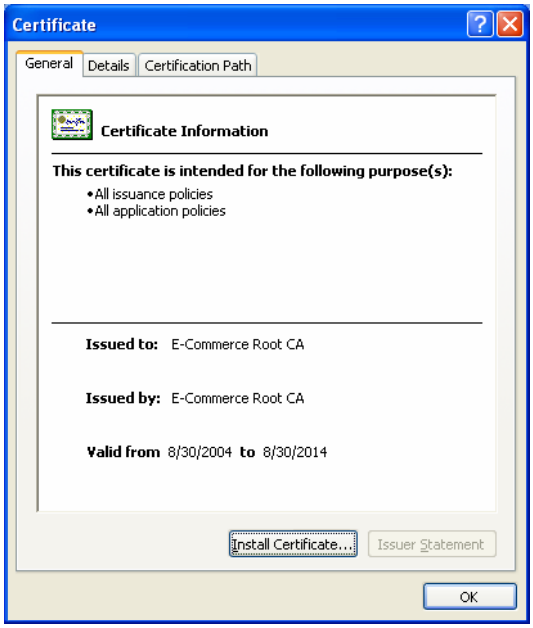
Root CA Certificate – Installation

The following steps are used to install the E-Commerce Root CA Certificate into the Internet Explorer Certificate Store.

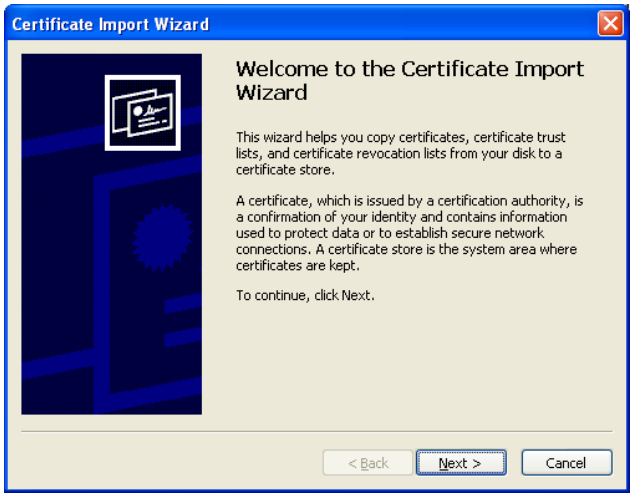
1. Access the Root CA Certificate link on the DEA E-Commerce Web site.
2. Click the link to **"Install the DEA E-Commerce Root CA Certificate"**.
3. At the prompt, click **Open**.



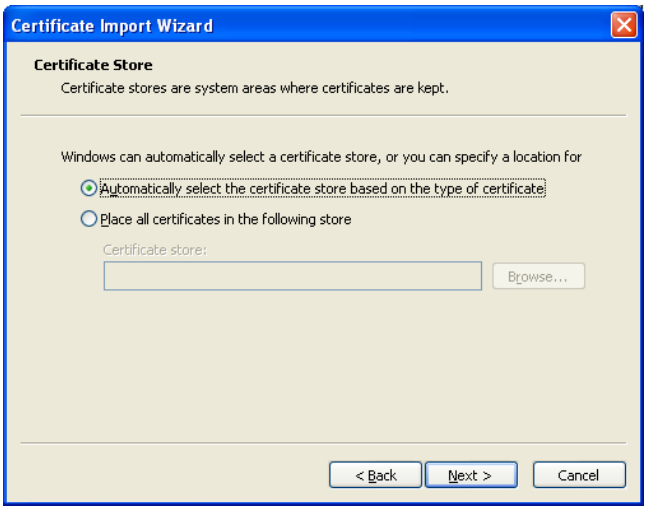
4. At the *Certificate* screen, click **Install Certificate**.



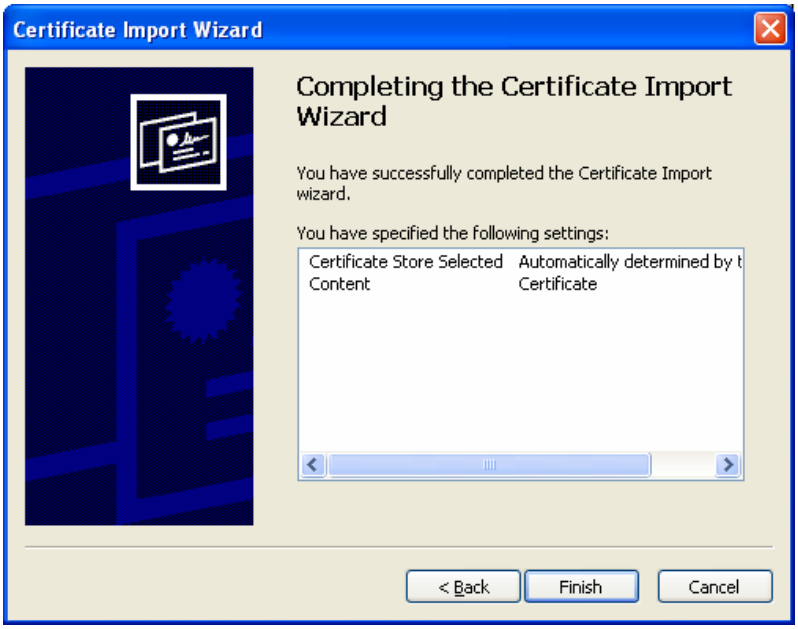
5. At the *Certificate Import Wizard* screen, click **Next**.



6. Verify that "Automatically select the certificate store based on the type of certificate" is selected and click **Next**.

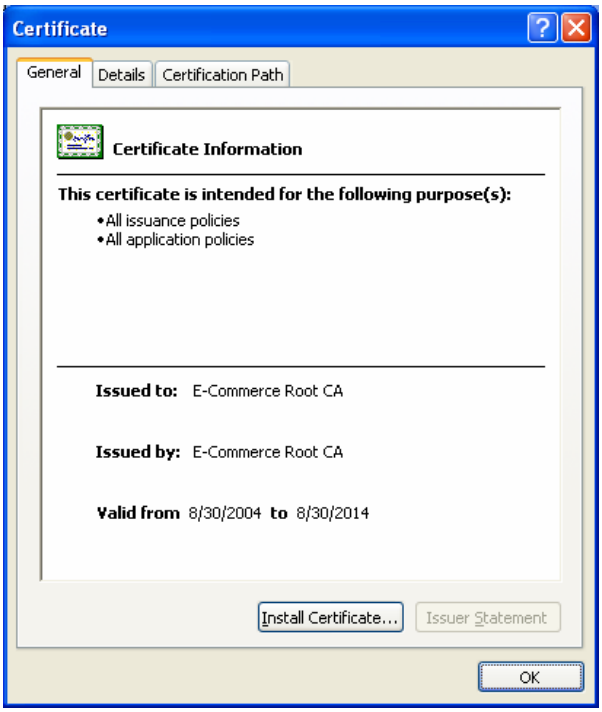


7. At the *Completing the Certificate Import Wizard* screen, click **Finish**.



8. At the *The import was successful* screen, click **OK**.

9. The import wizard returns to the *Certificate* screen. The certificate has been installed, so click **OK** to close the screen.



Root CA Certificate – Install Verification

All certificates installed using Internet Explorer are accessible through the Internet Explorer certificate store. The following steps are used to locate the Root CA Certificate in the certificate store. Once the Root CA Certificate is located, the installation of the Sub CA Certificate should be verified using the steps provided in the following section "CSOS Sub CA Certificate – Install Verification."

1. Open Internet Explorer.
2. At the top of the screen, select the **Tools** menu and click **Internet Options**.
3. In the Internet Options screen, switch to the **Content** tab.
4. On the Content tab, click the **Certificates** button.
5. The Root CA certificate is listed on the **Trusted Root Certificate Authorities** tab and is identified as being issued to "E-Commerce Root CA" and issued by "E-Commerce Root CA."

CSOS Sub CA Certificate – Where is it published?

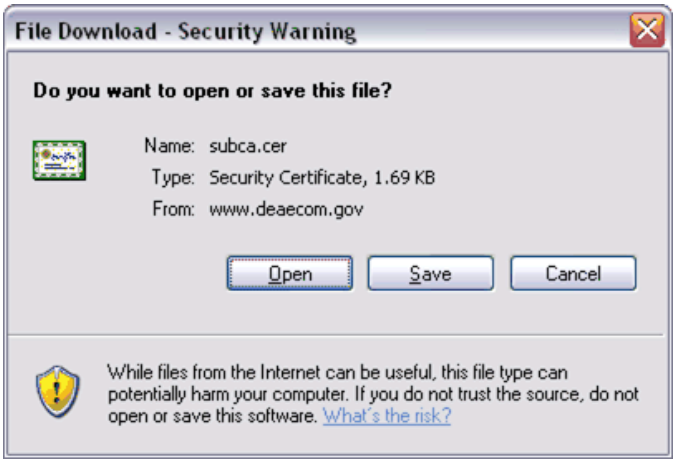
The Sub CA certificate may be found on the DEA E-Commerce Web site in one of two locations:

- In the Certificate Management section of the site
  - www.deaecom.gov/certmanage.html
- In the Certificate Retrieval section of the site
  - Private link provided to subscribers

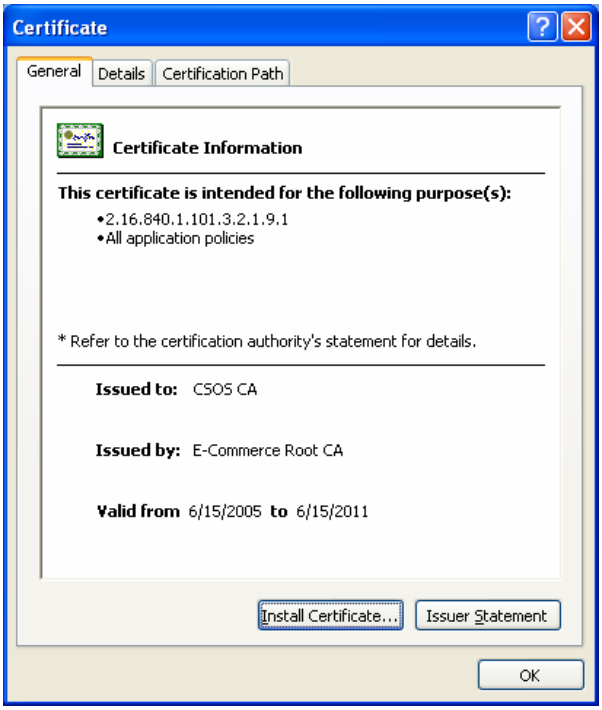
CSOS Sub CA Certificate – Installation

The following steps are used to install the CSOS Sub CA Certificate into the Internet Explorer Certificate Store.

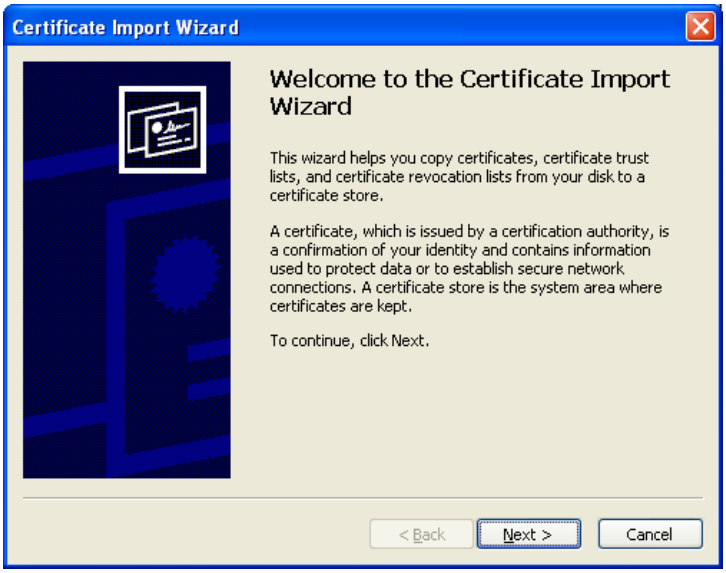
1. Access the Sub CA Certificate link on the DEA E-Commerce Web site.
2. Click the link to **"Install the CSOS Sub CA Certificate"**.
3. At the prompt, click **Open**.



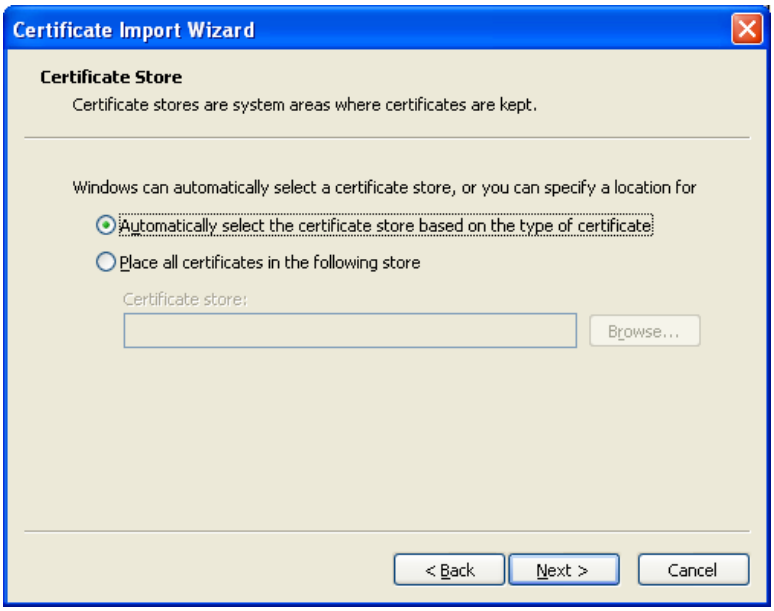
4. At the *Certificate* screen, click **Install Certificate**.



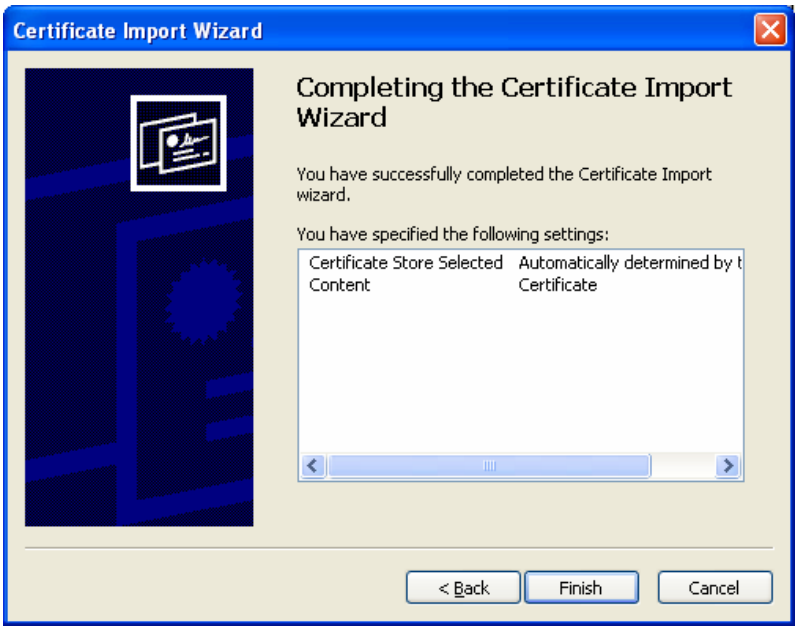
5. At the *Certificate Import Wizard* screen, click **Next**.



6. Verify that "Automatically select the certificate store based on the type of certificate" is selected and click **Next**.

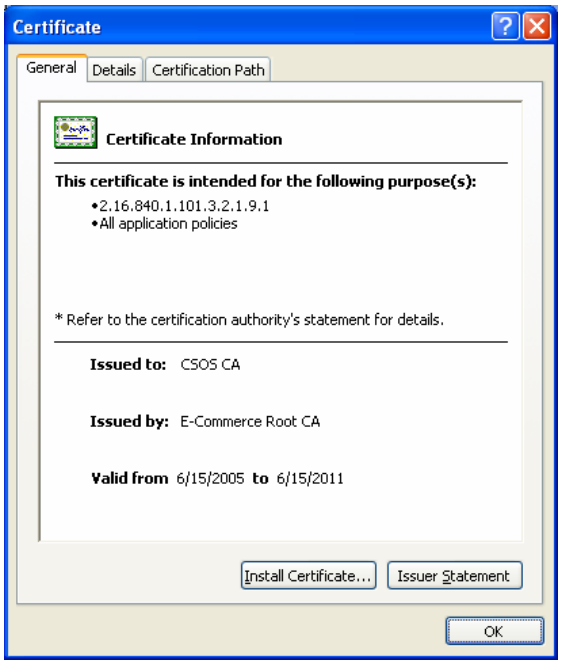


7. At the *Completing the Certificate Import Wizard* screen, click **Finish**.



8. At the *The import was successful* screen, click **OK**.

9. The import wizard returns to the *Certificate* screen. The certificate has been installed, so click **OK** to close the screen.



CSOS Sub CA Certificate – Install Verification

All certificates installed using Internet Explorer are accessible through the Internet Explorer certificate store. The following steps are used to locate the Sub CA certificate in the certificate store.

1. Open Internet Explorer.
2. At the top of the screen, select the **Tools** menu and click **Internet Options**.
3. In the Internet Options screen, switch to the **Content** tab.
4. On the Content tab, click the **Certificates** button.
5. The CSOS Sub CA certificate is listed on the **Intermediate Certificate Authorities** tab and is identified as being issued to "CSOS CA" and issued by "E-Commerce Root CA."

Netscape

The following instructions are specific to Netscape Browser version 8.1. Instructions for Internet Explorer are located in the previous section of this Guide.

Root CA Certificate – Where is it published?

The Root CA certificate may be found on the DEA E-Commerce Web site in one of two locations:

- In the Certificate Management section of the site
  - www.deaecom.gov/certmanage.html
- In the Certificate Retrieval section of the site
  - Private link provided to subscribers

Root CA Certificate – Installation

The following steps are used to install the E-Commerce Root CA Certificate into the Netscape Certificate Manager.

1. Access the Root CA Certificate link on the DEA E-Commerce Web site.
2. Click the link to **"Install the DEA E-Commerce Root CA Certificate"**.
3. At the *Downloading Certificate* screen, select all three check boxes and click **OK**.

- The following prompt will be displayed if the DEA E-Commerce Root CA Certificate is already installed in the Netscape Certificate Manager:

4. Netscape returns to the DEA E-Commerce Web site without confirmation of the certificate's installation.

Root CA Certificate – Install Verification

All certificates installed using Netscape Browser are accessible through the Netscape Certificate Manager. The following steps are used to locate the Root CA Certificate in the certificate store. Once the Root CA Certificate is located, the installation of the Sub CA Certificate should be verified using the steps provided in the following section "CSOS Sub CA Certificate – Install Verification."

1. At the top of the Netscape Browser, select Tools | **Options**.
2. Click on the **Advanced** button.
3. Scroll down the list and click on the **Manage Certificates** button.
4. Select the **Authorities** tab.
5. Scroll down to the "U.S. Government" section.
6. The CA certificates are listed in this section of the Certificate Manager.

CSOS Sub CA Certificate – Where is it published?

The Sub CA certificate may be found on the DEA E-Commerce Web site in one of two locations:

- In the Certificate Management section of the site
  - www.deaecom.gov/certmanage.html
- In the Certificate Retrieval section of the site
  - Private link provided to subscribers

CSOS Sub CA Certificate – Installation

The following steps are used to install the CSOS Sub CA Certificate into the Netscape Certificate Manager.

1. Access the Sub CA Certificate link on the DEA E-Commerce Web site.
2. Click the link to **"Install the CSOS Sub CA Certificate"**.

3. At the *Downloading Certificate* screen, select all three check boxes and click **OK**.

- The following prompt will be displayed if the Sub CA Certificate is already installed in the Netscape Certificate Manager:

4. Netscape returns to the DEA E-Commerce Web site without confirmation of the certificate's installation.

CSOS Sub CA Certificate – Install Verification

1. At the top of the Netscape Browser, select the *Tools* menu and click **Options**.
2. Click on the **Advanced** button.
3. Scroll down the list and click on the **Manage Certificates** button.
4. Select the **Authorities** tab.
5. Scroll down to the "U.S. Government" section.
6. The CA certificates are listed in this section of the Certificate Manager.

2. Subscriber Certificate Retrieval

Each CSOS certificate issued by DEA must be retrieved via the DEA E-Commerce Web site. Retrieval, which is synonymous with “activation” and “downloading”, is the process that creates the certificate and corresponding private key, and installs it in the Web browser’s certificate store.

- Each certificate may be retrieved only **once** and should be retrieved on the computer that the subscriber plans on using for placing controlled substance orders.

- Each CSOS certificate is issued to ***one individual subscriber***. This subscriber is the certificate “owner” and is the only person authorized to retrieve and use his/her certificate. Assistance with retrieval is allowed as long as the certificate owner is the only person who knows the certificate’s password. The certificate’s password is created during retrieval and is not known or provided by DEA.

- Certificates must never be retrieved without the certificate owner being present.

What information is needed for certificate retrieval?

Each certificate has a unique Access Code and Access Code Password pair that is required for retrieval. The Access Code is issued to the subscriber via E-mail. For security reasons, the Access Code Password is sent via U.S. Postal Mail to the subscriber's CSOS Coordinator for certificate's associated DEA Registration number and is then forwarded to the subscriber.

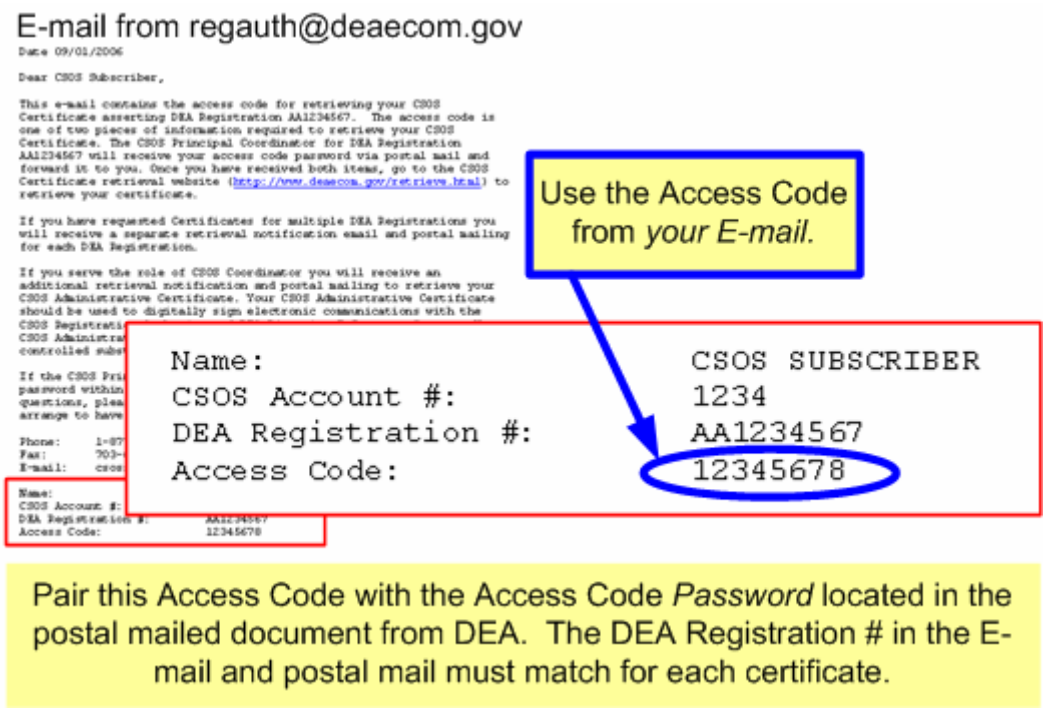
Access Codes (Via E-mail)

When a subscriber enrolls in the CSOS program, he/she is required to provide an E-mail address. This E-mail address is used by DEA to send each certificate's Access Code to the subscriber. Multiple E-mails/Access Codes will be issued for subscribers with more than one certificate. Each E-mail indicates:

- That the certificate is a CSOS Signing certificate. The E-mail will identify the DEA Registration number that the certificate is associated with (only for CSOS Signing certificates)
  - Each Certificate is specific to one individual and one DEA Registration

-or-

- That the certificate is a CSOS Administrative certificate



Sample E-mail activation notice with Access Code

Access Code Passwords (Via Postal Mail)

Each certificate's Access Code Password is indicated on its associated postal mailed activation notice from DEA. This notice is mailed to the Coordinator for the DEA Registration number at the mailing address provided on the Coordinator's enrollment application. Once the Coordinator verifies that he/she has authorized the individual for electronic ordering, the activation notice should be forwarded to the subscriber.

Each postal mail activation notice will indicate:

- That the certificate is a Signing certificate
  - Signing Certificate activation notices include the DEA Registration number associated with the certificate.

-or-

- That the certificate is an Administrative certificate
  - Administrative certificate activation notices contain an Admin Cert ID number rather than a DEA Registration number.

IMPORTANT INFORMATION ON ACTIVATING YOUR CSOS CERTIFICATE
Combine this information with the access code you received via E-Mail for this DEA Registration Number. **Please retain this document for future management of your certificate.**

DEA Diversion E-Commerce Support
E-Mail: csossupport@DEAecom.gov
Phone: 1-877-DEA-ECOM (1-877-332-3266)

Name:	**John Smith**
E-Mail address:	**John.Smith@Internet.com**
CSOS Account Number:	**0000**
Certificate Serial Number:	**R00002005001**
CA Thumbprint (SHA-1):	**FEBF F1A8 F348 4ABD A146 E64B 5760 21C7 AAAB 43AF**

Step 1 – Locate your E-Mail containing this same DEA Registration Number

DEA Registration Number:	**XX1234567**

Step 2 – Use this information to log in to the DEA E-Commerce Certificate Retrieval Web page

Web site Address:	**<Web site Address>**
Web site Username:	**<Web site Username>**
Web site Password:	**<Web site Password>**

Step 3 – Use this Access Code Password, along with the Access Code from your E-Mail to activate your certificate

Access Code Password:	**<Access Code Password>**

Sample postal mail activation notice with Access Code Password

System and Browser Requirements

Certificates must be retrieved using either Internet Explorer or Netscape Browser on a Windows Operating System. The Windows version must be Windows 98 or higher, but Windows 2000 or XP are strongly recommended.

Supported Browsers:

- Internet Explorer must be version 5 or higher
  - Use of the latest version (version 6) is strongly encouraged.
- Netscape Browser must be version 4.51 or higher
  - Use of the latest version (version 7 or 8) is strongly encouraged.

Non-Supported Browsers:

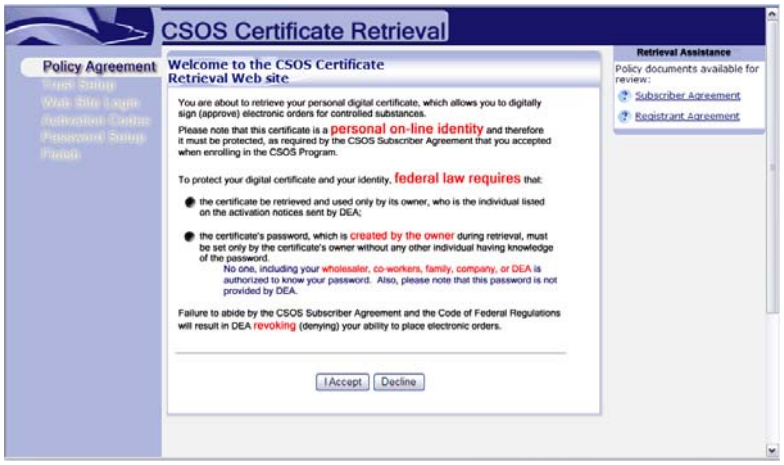
- AOL's browser, even when integrated with IE or Netscape, does not support certificate retrieval. AOL may be used to provide an Internet connection, however Internet Explorer or Netscape should be opened separately from AOL for certificate retrieval.
- MSN Browser *does not support* certificate retrieval.
- Mozilla Firefox *is not currently supported* by DEA for certificate retrieval.

Certificate Retrieval Instructions

Subscriber Certificate Retrieval – Internet Explorer

Access the CSOS Certificate Retrieval site. The address for this page is listed on both the certificate owner's E-mail and postal mailed activation notices.

Policy Agreement:
The ***owner*** of the certificate is required to review the following policy information and click **I Accept** to indicate that he/she understands and agrees to comply with the stated policy.



Trust Setup:
Install both the DEA E-Commerce Root CA and CSOS Sub CA certificates as documented on the side panel of the Web page and in the section of this Support Guide on CA certificates. These CA certificate installations are required once per ordering computer. If you are unsure whether the certificates have been installed, you may do so again since there is no harm in installing the CA certificates multiple times.

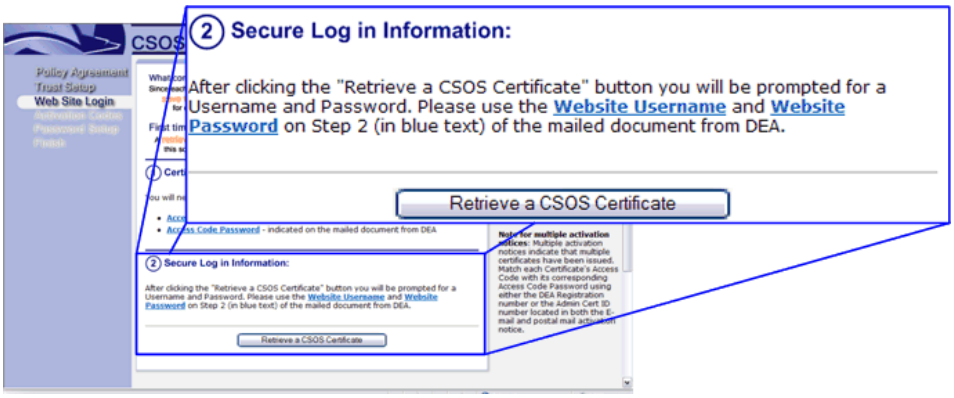
When finished, click the **Click to continue after installing both DEA CA Certificate** button at the bottom of the screen.

Web Site Login:

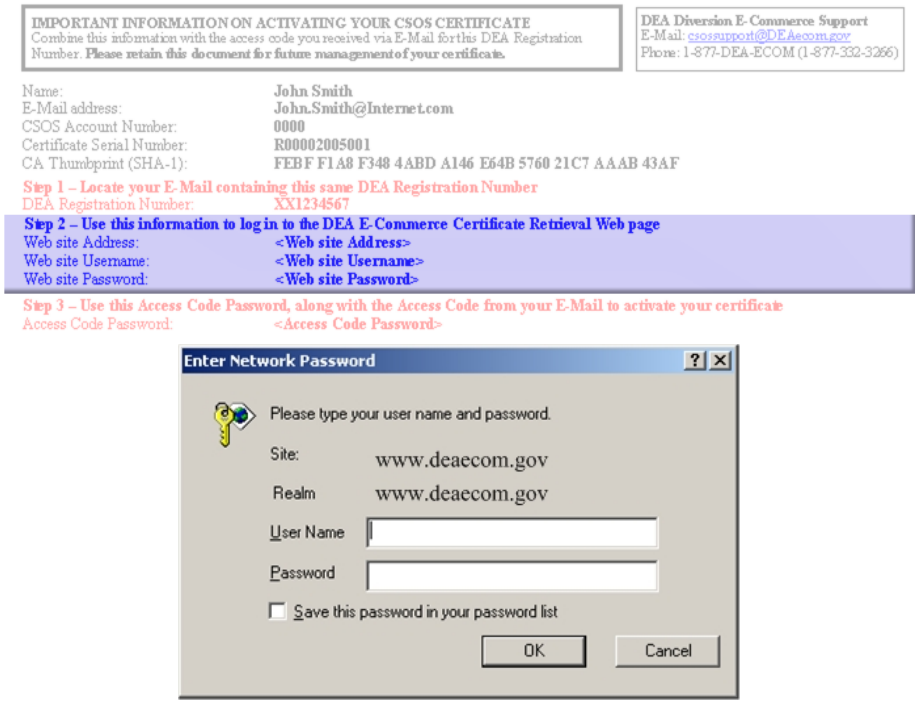
Step 1. Locate the Access Code and Access Code Password for the certificate. These codes will be entered on Step 3.

Step 2. Web site login:

a) Click the **Retrieve a CSOS Certificate** button.



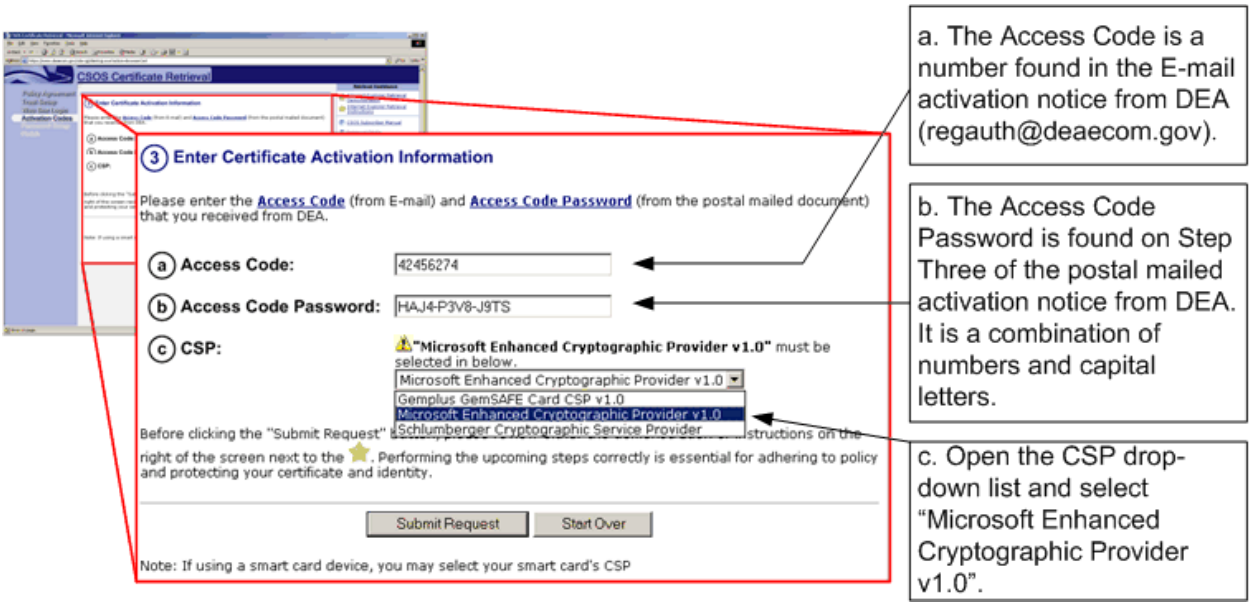
b) Enter the Web site User Name and Password located in Step 2 of the postal mailed document from DEA and click **OK**.



Tips:

- The Web Site Password is case sensitive.
- This requested password is not the Access Code Password from Step 3 of the mailed document from DEA.
- If you are positive that the username and password are being entered correctly, it is possible that the account has been locked out due to failed login attempts. Please call DEA Diversion E-Commerce Support (1-877-332-3266) if you suspect that the account has been locked out.

Step 3. Enter the certificate activation information:



a) **Enter the Access Code for this certificate**. The Access Code may be found in the E-mail from DEA (regauth@deaecom.gov) and is specific to this certificate only.

b) **Enter the Access Code Password for this certificate**. The Access Code Password may be found in Step 3 of the postal mailed document from DEA and is specific to this certificate only. The Access Code Password is a combination of numbers and letters separated by dashes (the dashes are optional).

c) **Select "Microsoft Enhanced Cryptographic Provider v1.0"** as the CSP. If not selected, the Web site will most likely indicate that an error has occurred.

- If Microsoft Enhanced Cryptographic Provider v1.0 is not selected as the CSP, the error 8010001D or 8010002E will occur as documented in the "Certificate Retrieval Error Codes" section of this Guide.

d) Click the **Submit Request** button.

Step 4. Click **Yes** to request the certificate.

- This prompt will not appear when using the latest version of Windows XP and Internet Explorer.

Step 5. The default security level is set to Medium. Click **Set Security Level** to change this level to **High**.

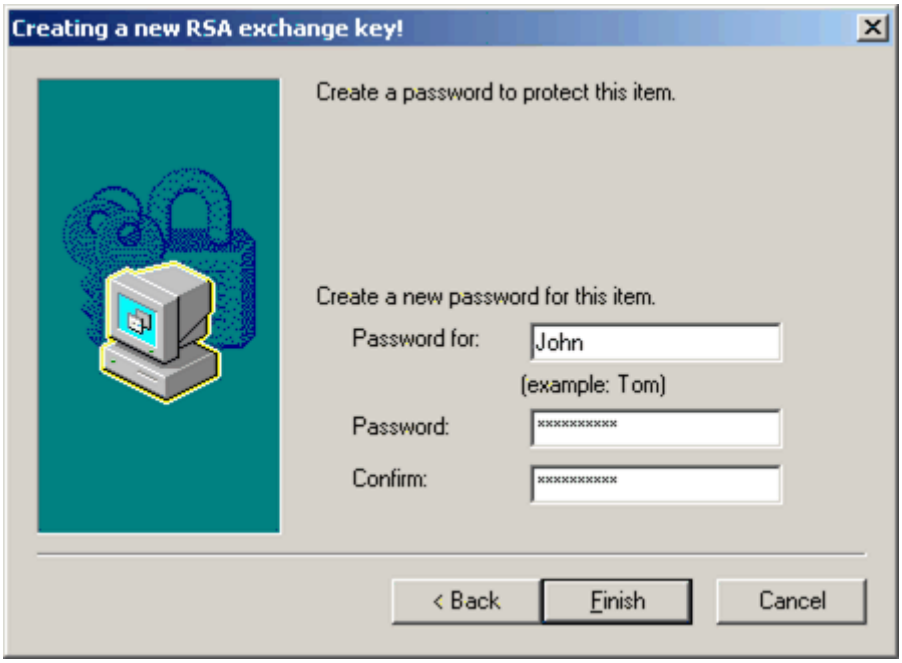
This is a ***required*** step for setting a private key password on the certificate. If this step is not performed, the certificate is vulnerable to being used by anyone who can acquire access to it. It is possible to set a password after a certificate has been retrieved (see the "Private Key Password Reset" section of this Guide).

Step 6. Select **High** and click **Next >**.

Step 7. Create a password for the certificate's private key and click **Finish**.

This information is to be entered and known by the owner of the certificate only! The owner of the certificate is the *individual* whose name appears on the inside of the postal mailed activation notice for this certificate. Knowledge of this password by any party other than the certificate owner, including a co-worker, spouse, or support representative, constitutes a private key compromise and the certificate is subject to revocation by DEA.

- Enter the name of the certificate owner in the **Password for** field.
  - The name does not need to be entered in any specific format.
  - This field is often grayed out and no information may be entered. This is OK.
- Create a password in the **Password** and **Confirm** fields.
  - The certificate owner must remember this password and may not share it with anyone.
  - A new certificate must be issued if this password is forgotten, lost, or compromised. Please stress this issue if working with a customer.
  - This password is CaSe SeNsItIvE, therefore the customer must be aware of any capitalization used when creating the password.
- When all fields are complete, click **Finish**.



Step 8. At the *An application is creating a Protected item* screen, click **OK**. Note that the screen now states, "Security level set to High."

Step 9. Click **Yes** at the *Potential Scripting Violation* prompt.

- This prompt may appear several times. You may click **Yes** to all prompts.
- This prompt may not appear when using the latest version of Windows XP and Internet Explorer.

Step 10. The following screen indicates that the certificate has been successfully retrieved.

Where is the certificate installed?

The retrieved certificate is installed in the Internet Explorer certificate store. The certificate may be accessed using the following steps:

1. At the top of the Internet Explorer screen, select the **Tools** menu and click **Internet Options**.
2. In the Internet Options screen, switch to the **Content** tab.
3. On the Content tab, click the **Certificates** button.
4. CSOS certificates are listed on the **Personal** tab and are identified as being issued by "CSOS CA."

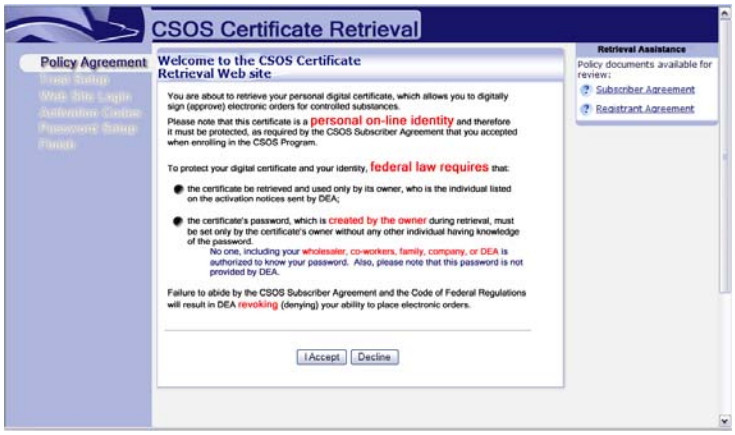
Subscriber Certificate Retrieval – Netscape

The following documentation was tested using Netscape Browser 8.1. Different versions of Netscape may behave differently from this documentation. Please contact DEA's E-Commerce Support Desk with any questions.

Access the CSOS Certificate Retrieval site. The address for this page is listed on both the certificate owner's E-mail and postal mailed activation notices.

Policy Agreement:

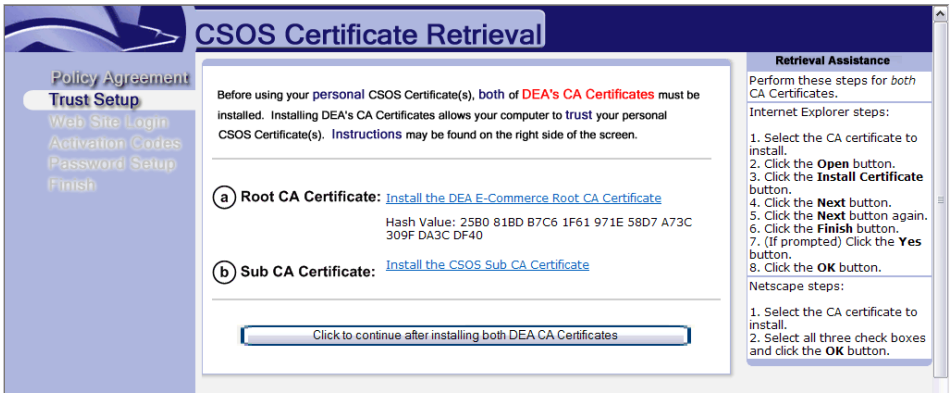
The ***owner*** of the certificate is required to review the following policy information and click **I Accept** to indicate that he/she understands and agrees to comply with the stated policy.



Trust Setup:

Install both the DEA E-Commerce Root CA and CSOS Sub CA certificates as documented on the side panel of the Web page and in the section of this Support Guide on CA certificates. These CA certificate installations are required once per ordering computer. If you are unsure whether the certificates have been installed, you may do so again since there is no harm in installing the CA certificates multiple times.

When finished, click the **Click to continue after installing both DEA CA Certificate** button at the bottom of the screen.

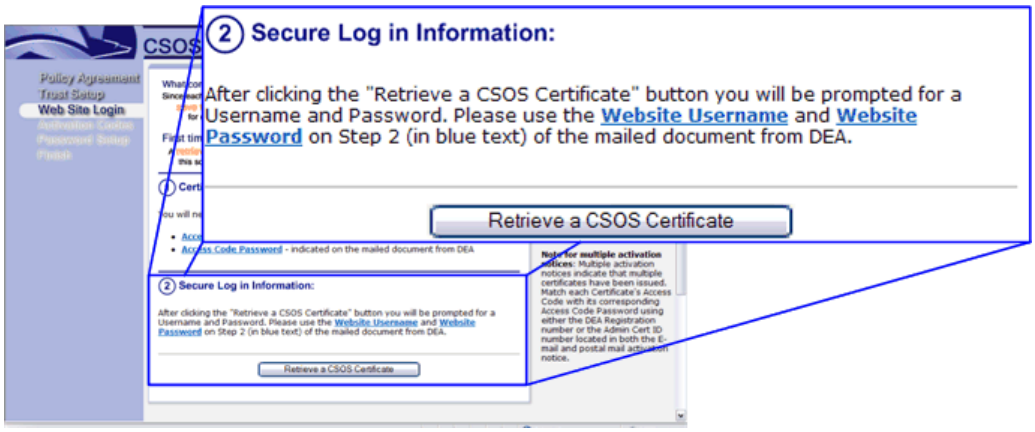


Web Site Login:

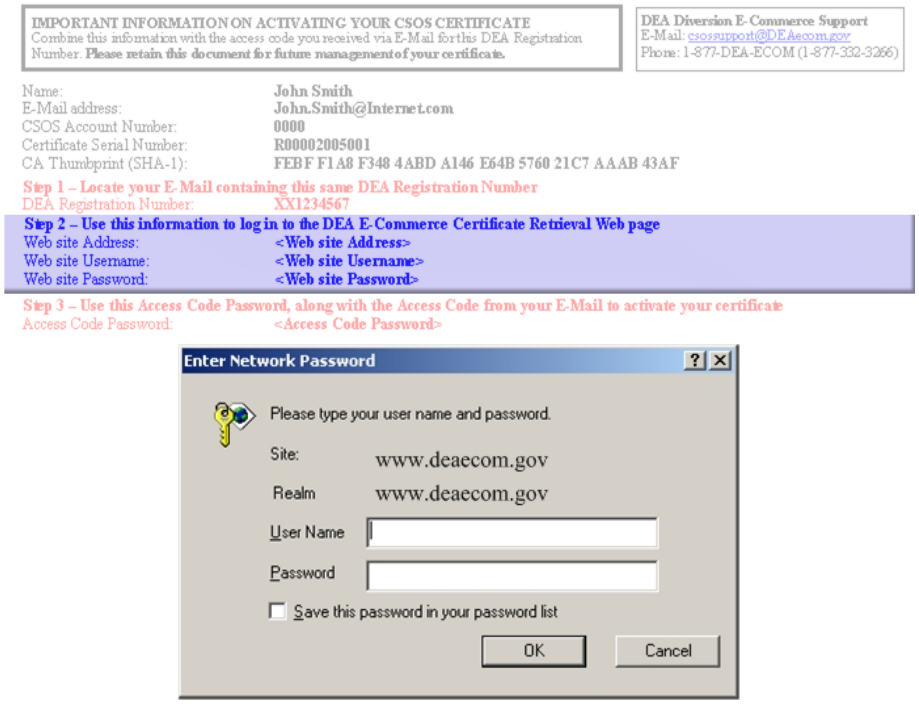
Step 1. Locate the Access Code and Access Code Password for the certificate. These codes will be entered on Step 3.

Step 2. Web site login:

a) Click the **Retrieve a CSOS Certificate** button.



b) Enter the Web site User Name and Password located in Step 2 of the postal mailed document from DEA and click **OK**.

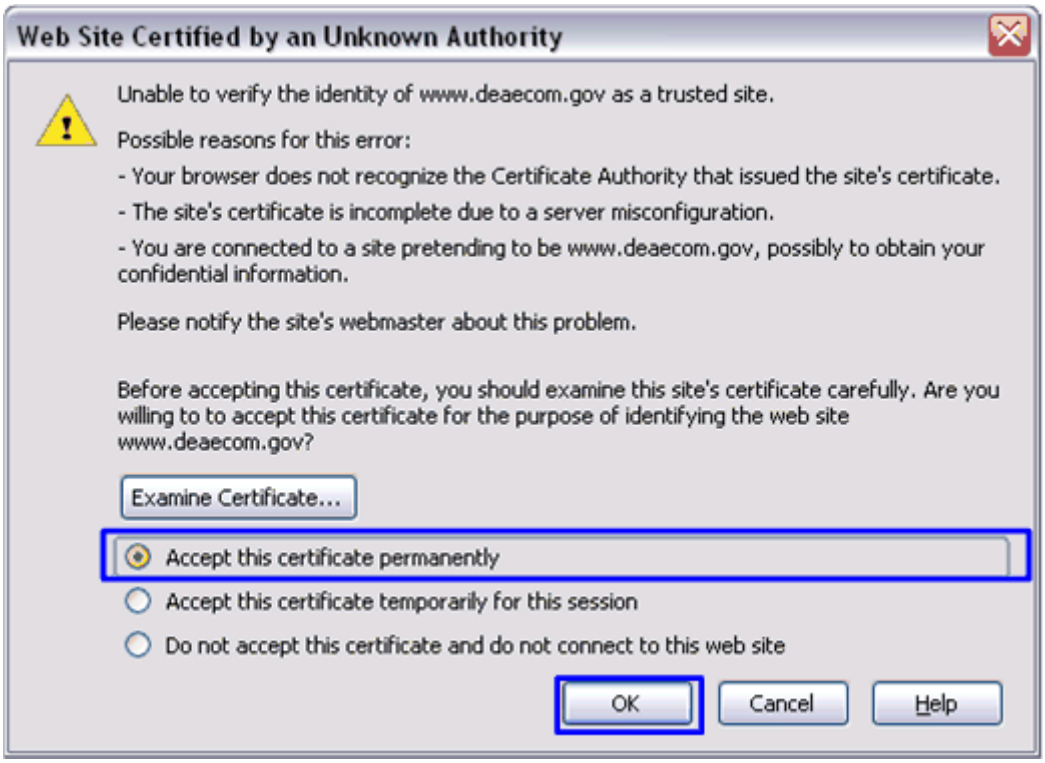


Tips:

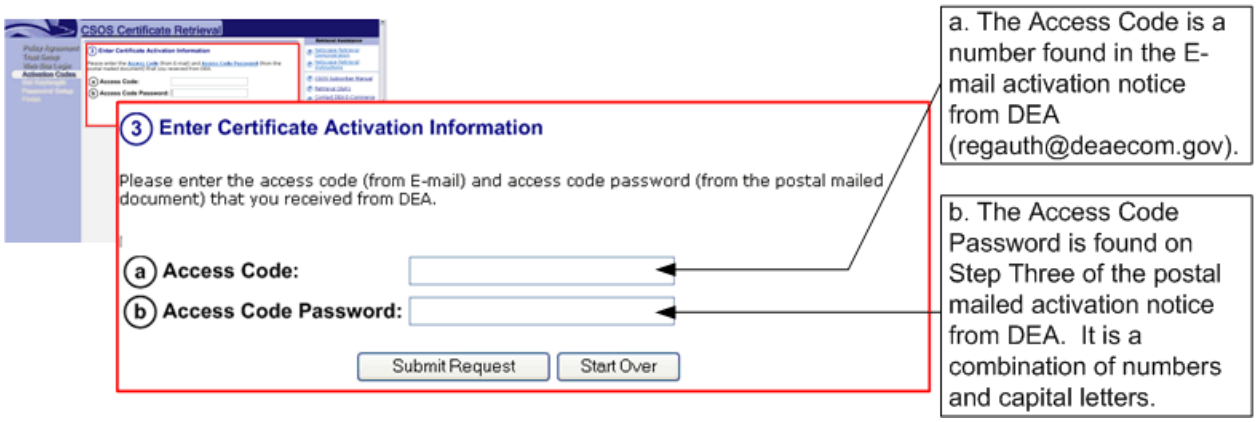
- The Web Site Password is case sensitive.
- This requested password is not the Access Code Password from Step 3 of the mailed document from DEA.
- If you are positive that the username and password are being entered correctly, it is possible that the account has been locked out due to failed login attempts. Please call

DEA Diversion E-Commerce Support (1-877-332-3266) if you suspect that the account has been locked out.

The following message will be displayed if the Web Certificate for the DEA E-Commerce Web site has not been installed on this system. Select the "Accept this certificate permanently" option and click **OK**.



Step 3. Enter the certificate's activation information.



Locate the **Access Code** in the E-mail sent by the DEA (regauth@DEAecom.gov).
Locate the CSOS user **Access Code Password** on the postal mailed document (shown below) from the DEA. Once entered, click the **Submit Request** button.

a) **Enter the Access Code for the certificate**. The Access Code may be found in the E-mail from DEA (regauth@deaecom.gov) and is specific to this certificate only.

b) **Enter the Access Code Password for this certificate**. The Access Code Password may be found in Step 3 of the postal mailed document from DEA and is specific to this certificate only.

IMPORTANT INFORMATION ON ACTIVATING YOUR CSOS CERTIFICATE
Combine this information with the access code you received via E-Mail for this DEA Registration Number. **Please retain this document for future management of your certificate.**

DEA Diversion E-Commerce Support
E-Mail: csossupport@DEAecom.gov
Phone: 1-877-DEA-ECOM (1-877-332-3266)

Name:	John Smith
E-Mail address:	John.Smith@Internet.com
CSOS Account Number:	0000
Certificate Serial Number:	R00002005001
CA Thumbprint (SHA-1):	FEBF F1A8 F348 4ABD A146 E64B 5760 21C7 AAAB 43AF

Step 1 – Locate your E-Mail containing this same DEA Registration Number

DEA Registration Number:	XX1234567

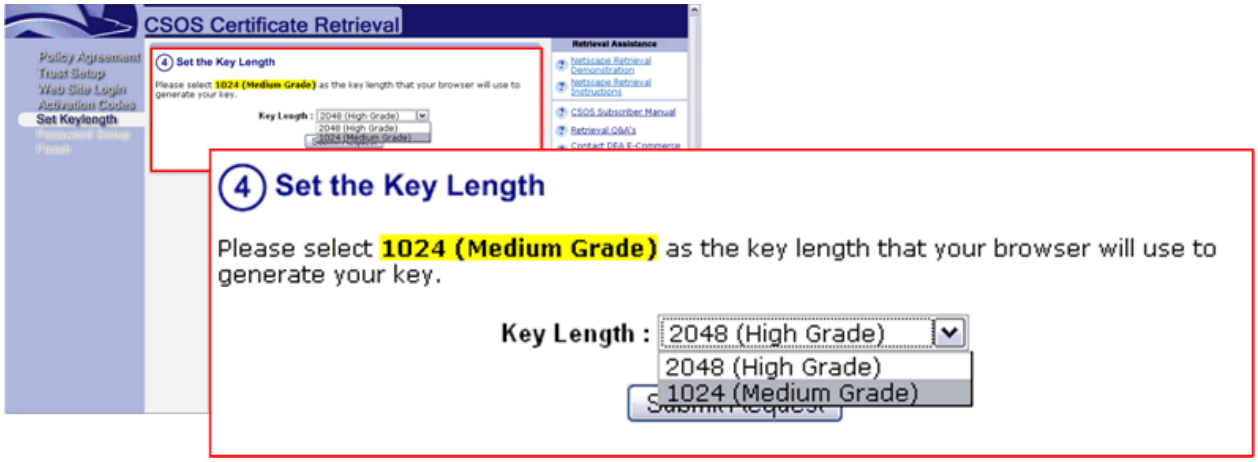
Step 2 – Use this information to log in to the DEA E-Commerce Certificate Retrieval Web page

Web site Address:	<Web site Address>
Web site Username:	<Web site Username>
Web site Password:	<Web site Password>

Step 3 – Use this Access Code Password, along with the Access Code from your E-Mail to activate your certificate

Access Code Password:	<Access Code Password>

Step 4. Select the certificate's key length. Set the key length drop-down list to 1024 (Medium Grade). Certificates activated at 2048 (High Grade) may be revoked due to incompatibility with some ordering systems. Once set to 1024 (Medium Grade), click the **Submit Request** button.

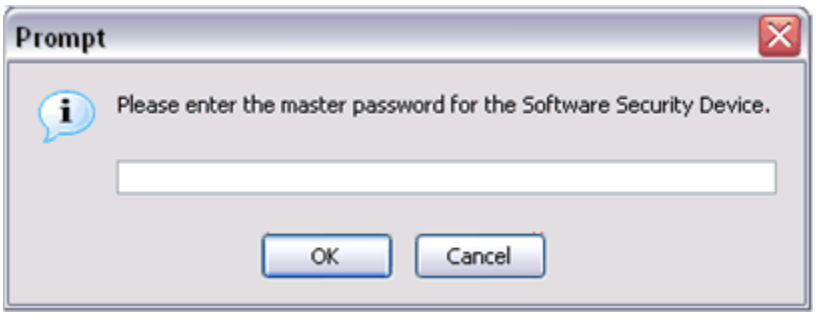


Step 5. Certificates retrieved using Netscape will be stored in the Netscape Software Security Device. Access to this Device is protected by a master password, which is specific to a Netscape user profile. One of the following two screens will appear. Please read the following instructions and click the **OK** button once finished.

a) If the Software Security Device has never been used, there will be no current password. The following screen appears, allowing the ***certificate owner*** to create a new password.

- The certificate owner must remember this password and may not share it with anyone.
- A new certificate must be issued if this password is forgotten, lost, or compromised. Please stress this issue if working with a customer.
- This password is CaSe SeNsItIvE, therefore the customer must be aware of any capitalization used when creating the password.

b) If the Software Security Device has been used before, the existing master password must be entered, or access will not be permitted.



Step 6. Please wait while the Certificate's private key is created.

The following screen indicates that the certificate has been successfully retrieved.

Where is the certificate installed?

The retrieved certificate is installed in the Netscape Certificate Manager. The certificate may be accessed using the steps documented in the "Finding Certificates" section of this Guide.

Certificate Retrieval Error Codes

Error –1666

Cause #1: The Certificate has already been retrieved. Each certificate may only be retrieved once.

Resolution #1:

- Check for the certificate in the certificate store on *all* computers that the user may have attempted activation.
  - Verify which browsers may have been used (i.e. Internet Explorer, Netscape, Mozilla Firefox).
  - Verify whether multiple Windows accounts are used to log in to the computer.
- If the certificate cannot be found, contact DEA Diversion E-Commerce Support immediately:
  - DEA will be able to determine if the certificate was activated and can provide the date and time it was activated.

Cause #2: The Access Code and/or Access Code Password have been entered incorrectly. Typically, an incorrect Access Code or Access Code Password will result in error 3274 or 3290. However, this error (-1666) may be the result of an incorrect access code and/or password.

Resolution #2: In this case, have the subscriber re-enter his/her access code and password (see resolution for 3274 and 3290). Additionally, the CSOS CA can assist the customer with retrieval and verify whether the Access Code and/or Access Code Password are correct.

Cause #3: The certificate's activation information has expired. Activation information (i.e. the Access Code and Access Code Password) is valid for 60 days from the date indicated on the top right corner of the postal mailed document.

Resolution #3: Contact DEA Diversion E-Commerce Support to have the codes reissued.

Cause #4: Transmission error/unsuccessful certificate creation. The CSOS CA recognizes the certificate as being retrieved, but the subscriber's system did not successfully create the certificate. Since the CSOS CA has the certificate as being retrieved, the customer *will not* be able to retrieve this certificate again.

Resolution #4: Contact DEA Diversion E-Commerce Support to troubleshoot the issue. If all other causes are ruled out *by DEA*, the certificate will need to be revoked and reissued. Revocation is a last resort and requires the owner of the certificate to contact DEA Diversion E-Commerce Support. No other party is authorized to request that a certificate be revoked.

Error 2278

Cause: The certificate is expired (not the activation codes, but the actual certificate). CSOS Signing certificates are set to expire when their associated DEA Registration number expires. The expiration date of the certificate is acquired from DEA records at the time the certificate is *issued*, which may be up to two months before the certificate is actually activated. Also, if a DEA Registration is renewed, it is possible that the CSOS CA records were not updated immediately.

Resolution: This certificate *will not* retrievable until the CSOS CA has updated the expiration date. Call DEA Diversion E-Commerce Support at 1-877-332-3266. If the DEA Registration has been renewed, the certificate expiration date will be updated. Only after the expiration date is updated will the certificate be retrievable.

Error 2731

Cause: There is a space at the end of an otherwise correct Access Code or Access Code Password. This would typically occur if the Access Code is copied from the activation E-mail and pasted into the Access Code box on the Web site rather than being typed.

Resolution: Click the **Back** button on the browser and remove any extra spaces at the end of both the Access Code and/or Access Code Password.

Error 3274

Cause: The Access Code and Access Code Password are probably valid, but are not a correct pair. Each certificate has a unique Access Code and Access Code Password. If a customer has received multiple certificates (indicated by multiple mailed documents), then the codes being entered are not for the same certificate.

Resolution: The Access Code from the activation E-mail corresponds to only one postal mailed Access Code Password. These codes may be matched correctly by determining which activation notices are for the Administrative certificate or by matching DEA Registration numbers from both notices for the signing certificate.

Related cause: All activation notices may not be present. It is possible for only one E-mail to arrive while any other required E-mails are automatically deleted by the E-mail software. Additionally, postal mailed activation notices are always mailed on the same day, but may be separated in the mail and arrive on separate days.

Related resolution:

- Missing postal mail activation notice
  - Mailed notices may arrive up to several days apart, please wait for the next notice.
  - If the subscriber has received activation E-mails, please wait at least 7 days for the postal mailed notice to arrive.
  - After waiting a sufficient amount of time, contact DEA Diversion E-Commerce Support to have the notice(s) re-sent.
- Missing E-mail
  - Check the E-mail client's SPAM or Junk Mail folder. The E-mail is originally sent on the same date as is indicated on the top right corner of the postal mailed document.
  - Guess the Access Code based on an E-mail that did arrive; Access Codes are sequential with the signing certificate usually being first. Typically, but not always, the Administrative certificate Access Code will be one digit higher than the Access Code for the Signing certificate.
  - Contact DEA Diversion E-Commerce Support to have the E-mail(s) re-sent.

Error 3290

Cause: Either the Access Code or Access Code Password has been incorrectly entered. Typically this is due to a simple typo.

Resolution: Click the **Back** button on the browser and review the Access Code and Access Code Password for typos. If there is a zero in the Access Code Password, change the zero to a capital letter 'O'. Also, verify that the Access Code and Access Code Password have been entered into the correct fields and are not swapped (i.e. the Access Code should be all numbers, the Access

Code Password should be the long string of numbers and letters with dashes). Also verify that the Web site password is not being entered as the Access Code Password.

Error 8010001D or 8010002E

Cause: Microsoft Enhanced Cryptographic Provider v1.0 was not selected as the CSP (Cryptographic Service Provider). A variety of similar error numbers may occur.

Resolution:

1. Click **OK** to the error message.
2. Click the browser's **Back** button to return to the screen where the with the Access Code and Access Code Password.
3. Change the CSP and click **Submit Request**.
   - If no CSP options are available, see section "No providers are listed in the CSP dropdown list."
4. Proceed with the standard steps for retrieving the certificate.

No key pair has been generated (no error number)

Cause #1: The subscriber may be using AOL or MSN Browser.

Resolution #1: Have the subscriber open and use Internet Explorer or Netscape.

Cause #2: There may be an issue with the Access Code, Access Code Password, or CSP selection.

Resolution #2:

1. Click the browser's **Back** button.
2. Have the subscriber attempt to activate again, this time verifying that the Access Code and Access Code Password are correct, and that the CSP field is set to *Microsoft Enhanced Cryptographic Provider v1.0*.

Cause #3: Unknown technical issues with the subscriber's computer.

Resolution #3: Attempt to activate on a different computer, export the certificate, and transfer it to the ordering computer.

No providers are listed in the CSP dropdown list

The CSP dropdown list should include all available CSPs on the current computer. However, due to security restrictions or corrupt/missing CSP files, no CSPs are available for certificate retrieval. Two workarounds are available:

1. Retrieve the certificate(s) on a different computer. The retrieved certificate(s) may then be transferred to any computer (including the original computer with the CSP issue) using the procedures outlined in the "Certificate Transfer" section of this Guide.
2. If no other computer is available, Netscape Browser may be installed for free from www.netscape.com. Netscape Browser has a build in CSP and will be able to successfully retrieve the certificate(s).

3. Certificate Management

Where are certificates installed?

Certificates are installed, by default, in the certificate store of the Web browser being used for retrieval. This means that certificates retrieved using Internet Explorer can be found:

- On the computer used to retrieve the certificate
- On the Windows system account (i.e. Windows log-in user name) used for retrieval
  - This bullet is not applicable if only one system account is used or if accounts are not used.
- In Internet Explorer

The same holds true for subscribers who use Netscape or Mozilla Firefox. Certificates retrieved using Netscape or Firefox *will not* be found in the Internet Explorer certificate store unless they are transferred to it.

Finding certificates

Certificates may be found in a number of locations. Certificates will typically be found in the certificate store as described in the previous section. If the certificate is not found in the certificate store, some troubleshooting may be required.

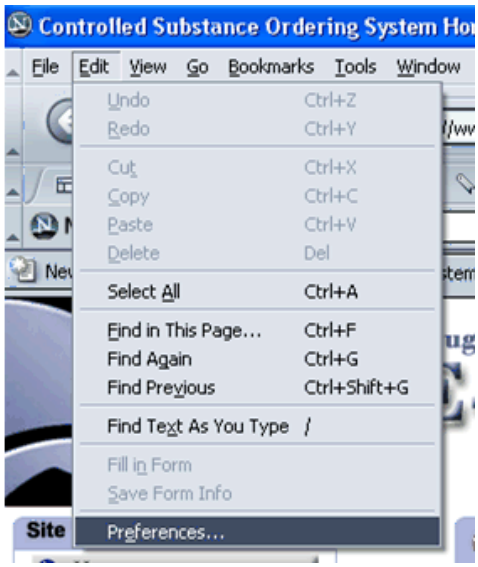
Locating certificates in Internet Explorer

1. Open Internet Explorer.
2. At the top of the screen, select the **Tools** menu and click **Internet Options**.
   - If Tools | Internet Options does not exist in Internet Explorer or is not accessible due to security restrictions, then Internet Options *may* be accessible through the Windows Control Panel in the Start Menu.
3. In the Internet Options screen, switch to the **Content** tab.
4. On the Content tab, click the **Certificates** button.
5. CSOS certificates are listed on the **Personal** tab and are identified as being issued by "CSOS CA."

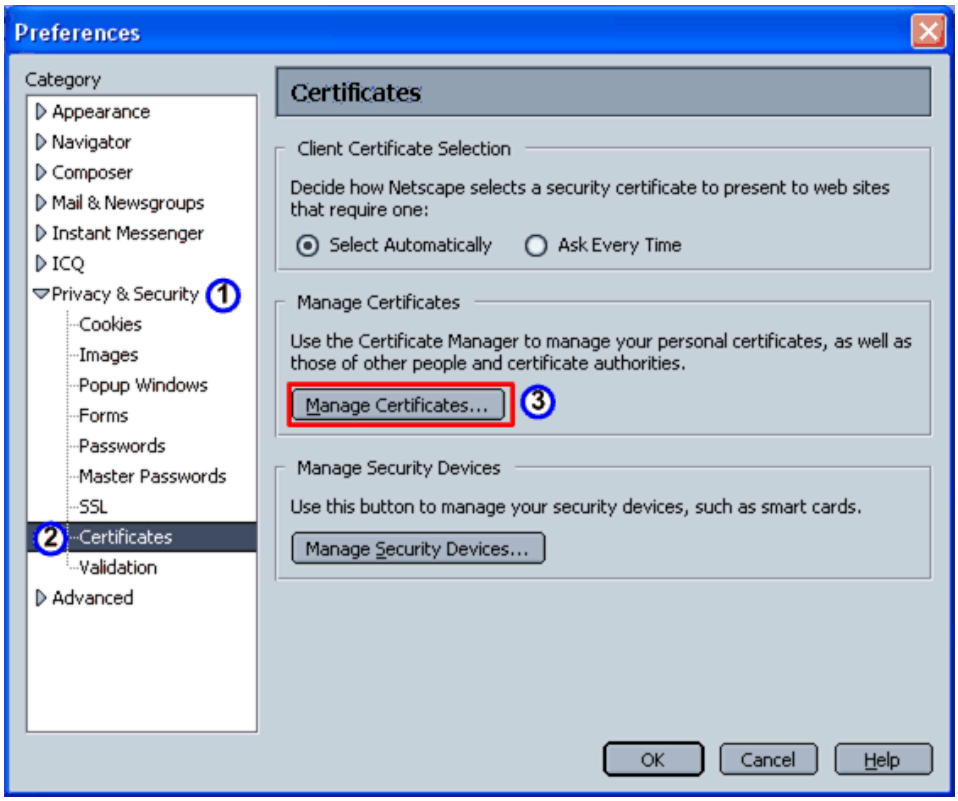
Locating certificates in Netscape 7.2

The version of Netscape Browser may be determined by selecting the Help menu and clicking the **About** option.

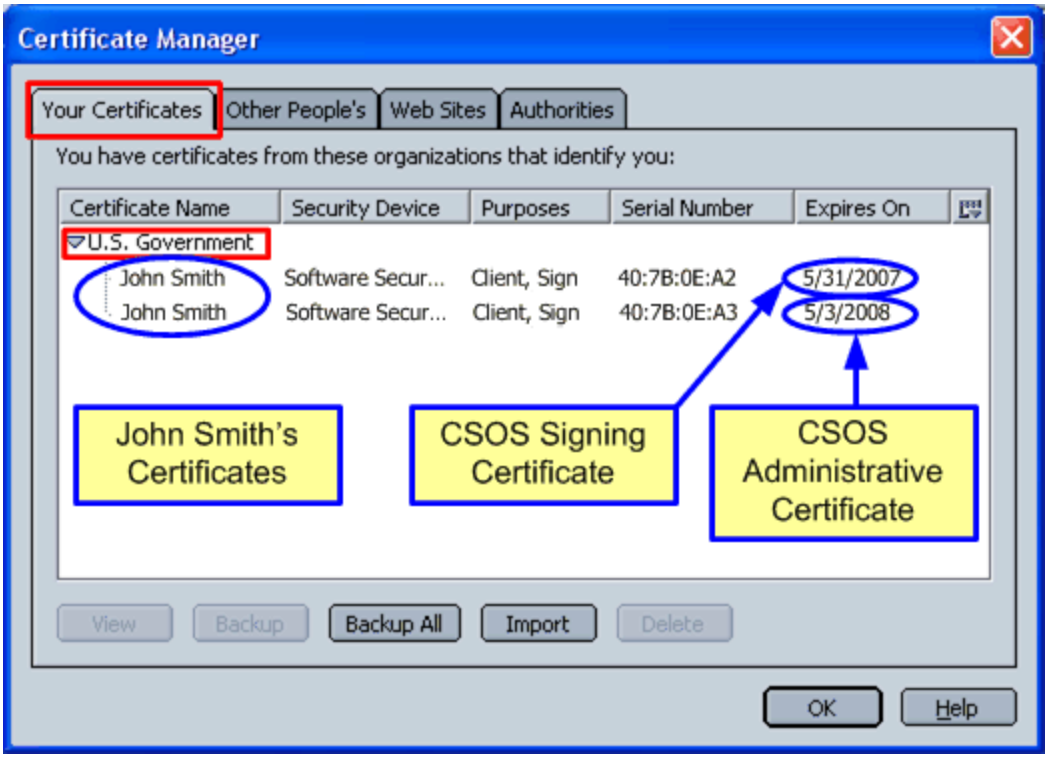
1. Open the *Edit* menu and select **Preferences…**



2. In the *Preferences* screen, select and expand the *Privacy & Security* category on the left of the screen (1). In the *Privacy & Security* category, select *Certificates* (2). Click the **Manage Certificates…** button (3).



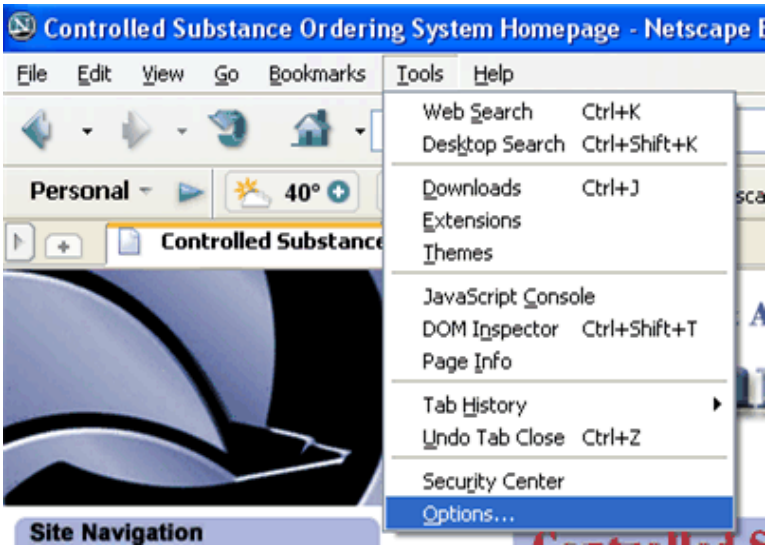
3. The *Certificate Manager* screen opens. All CSOS subscriber certificates (Administrative and Signing) are located on the *Personal* tab in the *U.S. Government* section.
   - The certificate owner's name appears as the Certificate Name.
   - **Administrative certificates** expire three years from the date issued.
   - **Signing certificates** expire when the associated DEA Registration expires.
     - This date will typically be earlier than the date for the Administrative certificate.
     - This date will always be at the end of the month.



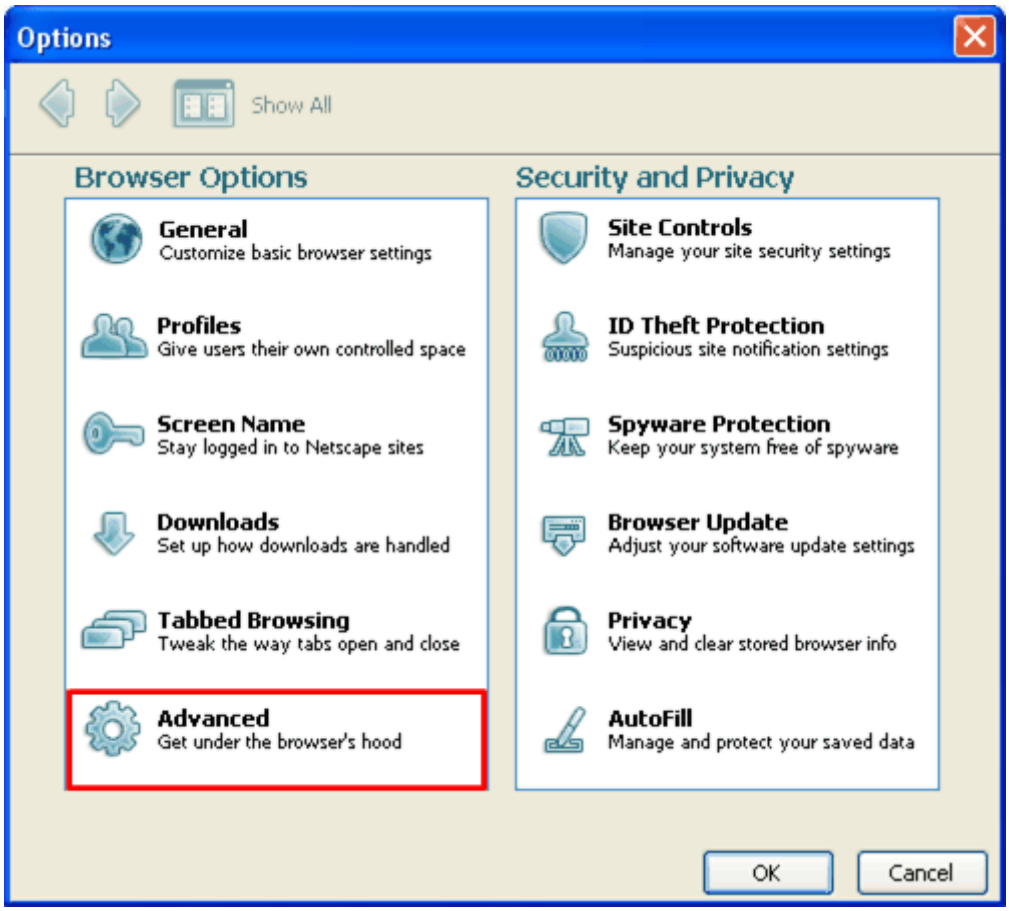
Locating certificates in Netscape 8.1

The version of Netscape Browser may be determined by selecting the Help menu and clicking the **About** option.

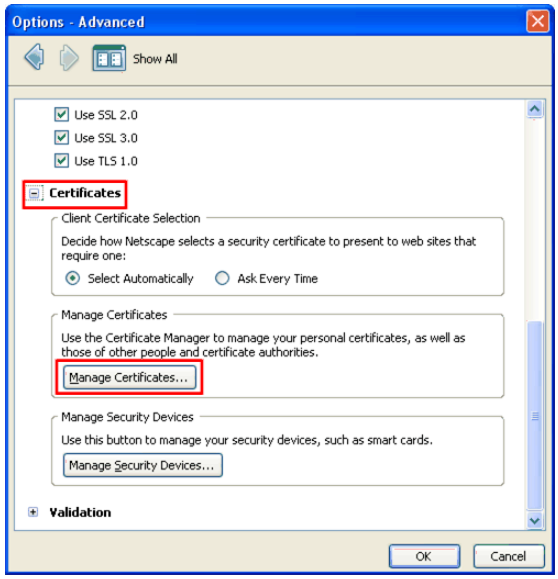
1. Open the *Tools* menu and select **Options…**



2. In the *Options* menu click **Advanced**.

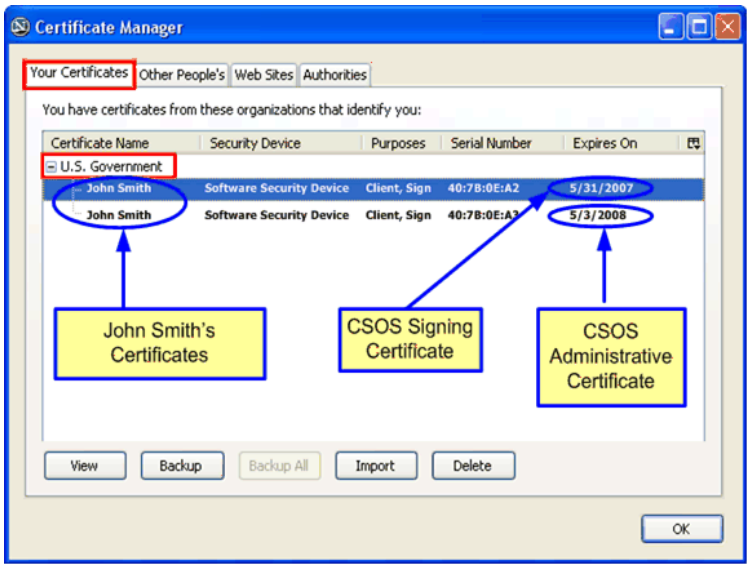


3. On the *Options-Advanced* screen scroll down to the section on Certificates. This section may need to be expanded by clicking the +. In the *Certificates* section click the **Manage Certificates** button.



4. The *Certificate Manager* screen opens. All CSOS Subscriber Certificates (Administrative and Signing) are located on the *Personal* tab in the *U.S. Government* section.

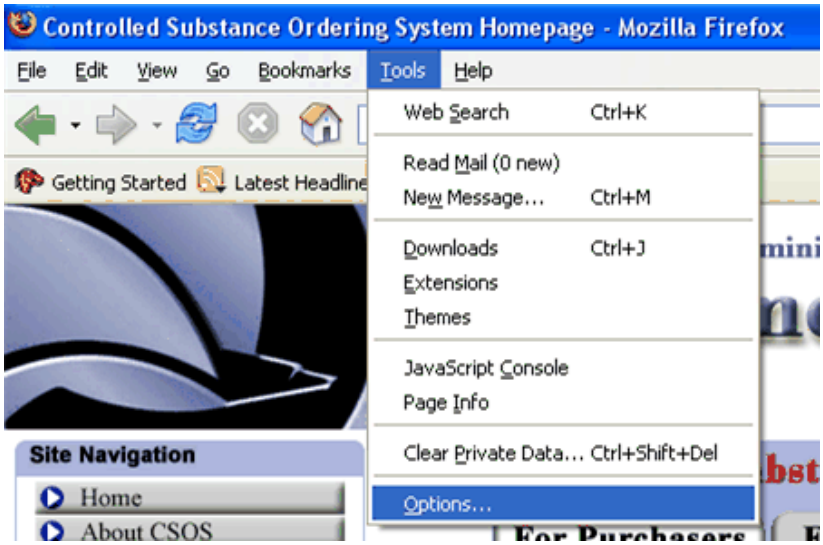
   - The certificate owner's name appears as the Certificate Name.
   - **Administrative certificates** expire three years from the date issued.
   - **Signing certificates** expire when the associated DEA Registration expires.
     - This date will typically be earlier than the date for the Administrative certificate.
     - This date will always be at the end of the month.



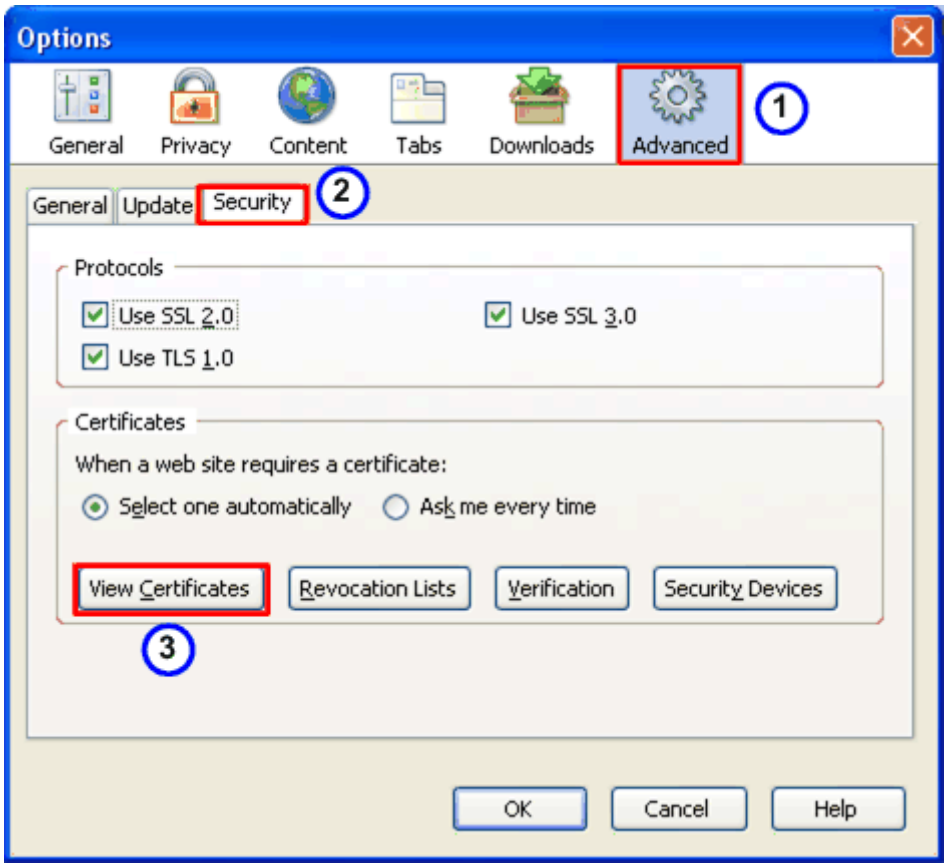
Locating certificates in Mozilla Firefox 1.5

The version of Mozilla Firefox may be determined by selecting the Help menu and clicking the **About** option.

1. Open the *Tools* menu and select **Options…**



2. In the *Options* menu click **Advanced** (1). On the *Security* tab (2), click the **View Certificates…** button (3).



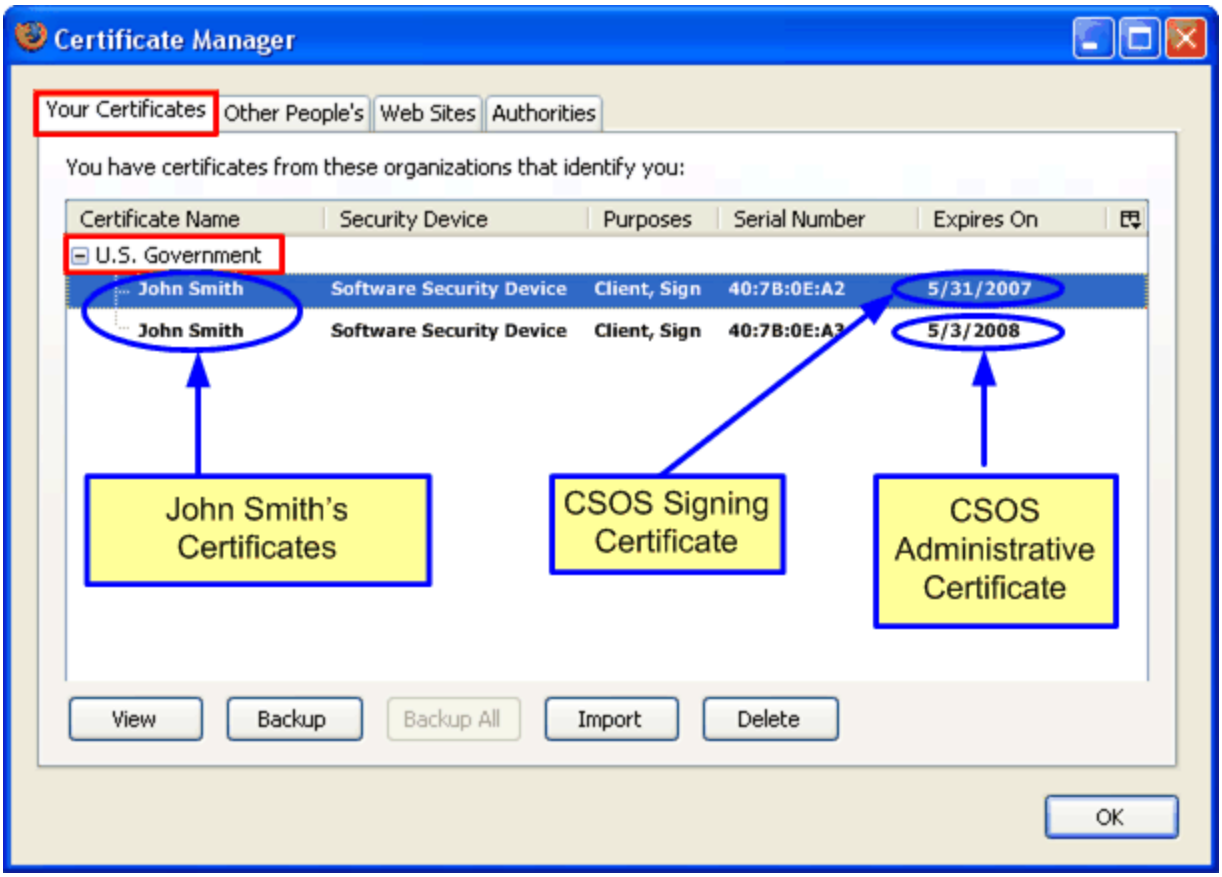
3. The *Certificate Manager* screen opens. All CSOS Subscriber Certificates (Administrative and Signing) are located on the *Personal* tab in the *U.S. Government* section.

   The certificate owner's name appears as the Certificate Name.

   Administrative certificates expire three years from the date issued.

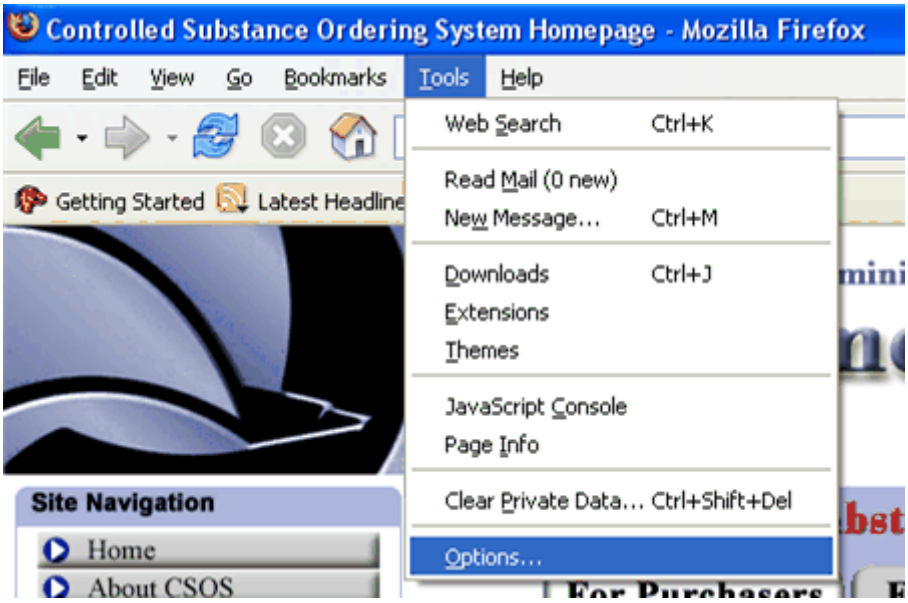
   Signing certificates expire when the associated DEA Registration expires.

   - This date will typically be earlier than the date for the Administrative certificate.
   - This date will always be at the end of the month.

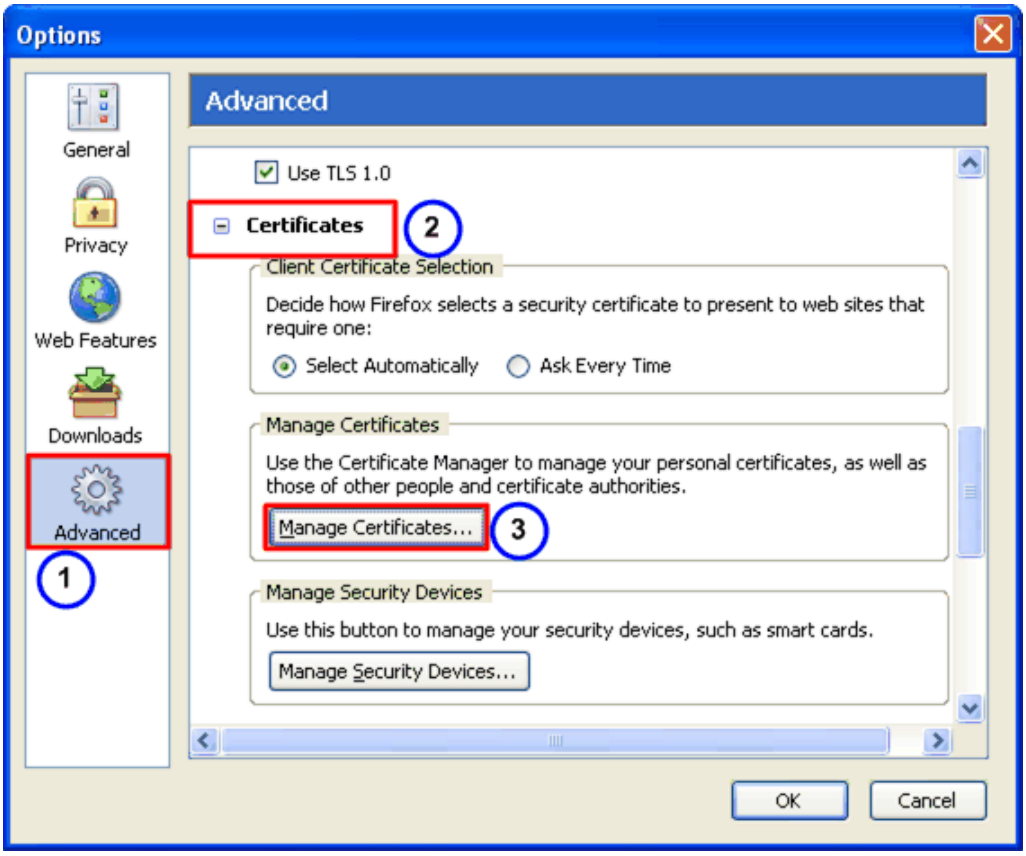


Locating certificates in Mozilla Firefox 1.0

1. Open the *Tools* menu and select **Options…**



2. In the *Options* menu click *Advanced* (1). Expand the *Certificates* category (2), and then click the **Manage Certificates…** button (3).



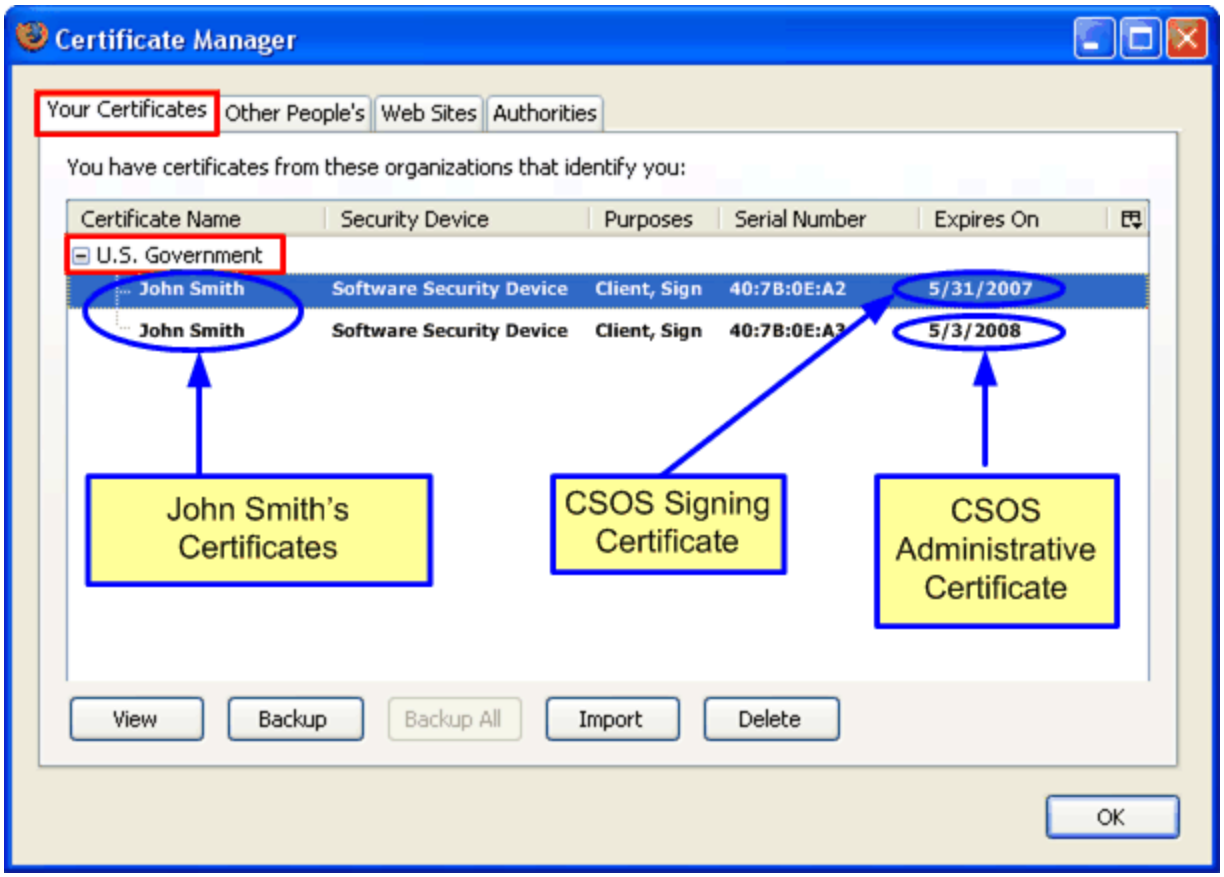
3. The *Certificate Manager* screen opens. All CSOS subscriber certificates (Administrative and Signing) are located on the *Personal* tab in the *U.S. Government* section.

   The certificate owner's name appears as the Certificate Name.

   Administrative certificates expire three years from the date issued.

   Signing certificates expire when the associated DEA Registration expires.

   - This date will typically be earlier than the date for the Administrative certificate.
   - This date will always be at the end of the month.



What to do if the certificate is not found in a browser

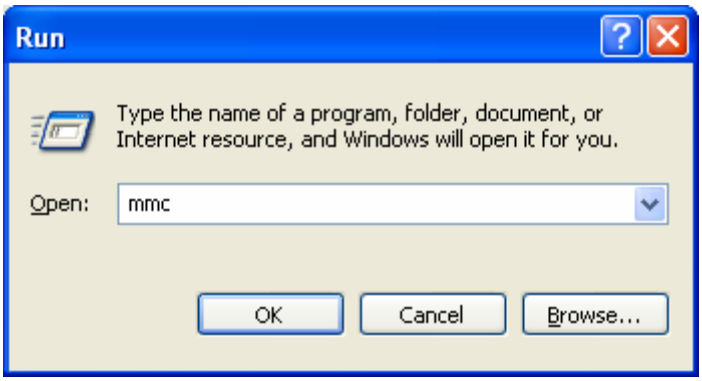
- The certificate may have been installed using a ***different browser***
  - Ask the customer whether it is possible that Netscape or Firefox were used
- The certificate may have been installed using a ***different computer***
  - Ask the customer whether anyone has *attempted* to enter the Access Code and Access Code Password on the DEA E-Commerce Web site using a different computer
  - If this is the case, then the certificate will need to be transferred. Certificates may only be activated once, but may be transferred from one computer to another. Certificate transfer steps are contained in this Guide (see table of contents)
- The certificate may have been installed using a ***different Windows account***
  - Ask the customer if there are multiple Windows accounts that log into the computer
  - If this is the case, log in using the other account and export the certificate to the C:\ drive where it may be accessed by all users.
- The certificate may have been removed from the certificate store
  - Search the computer for PFX files – see section "Locating certificate files"
  - Check the Microsoft Management Console (MMC) – see section "Locating certificates in the Microsoft Management Console (MMC)"

Locating certificates in the Microsoft Management Console (MMC)

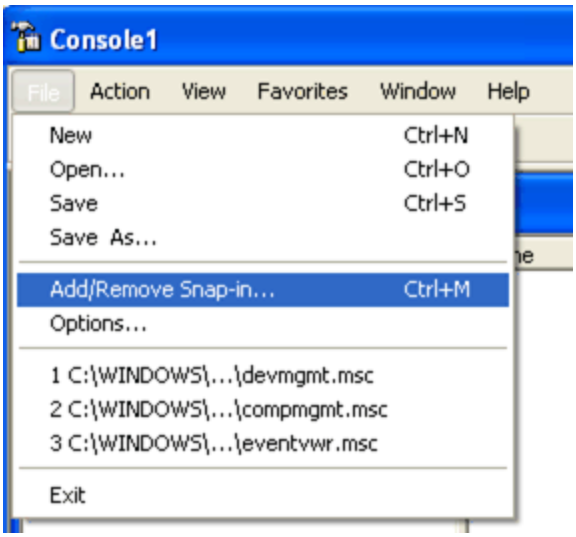
Certificates may be accessed in the MMC in addition to the Internet Explorer certificate store. On rare occasions (typically due to IE permission/security issues) a certificate may be found in the MMC and not IE. Certificates that are not installed in a certificates store (i.e. only existing as *.pfx or *.p12 certificate files) or are installed only in a Netscape or Firefox browser will not appear in the MMC.

Note: Windows 98 may not have the MMC installed. The MMC application may be downloaded from Microsoft's Web site.

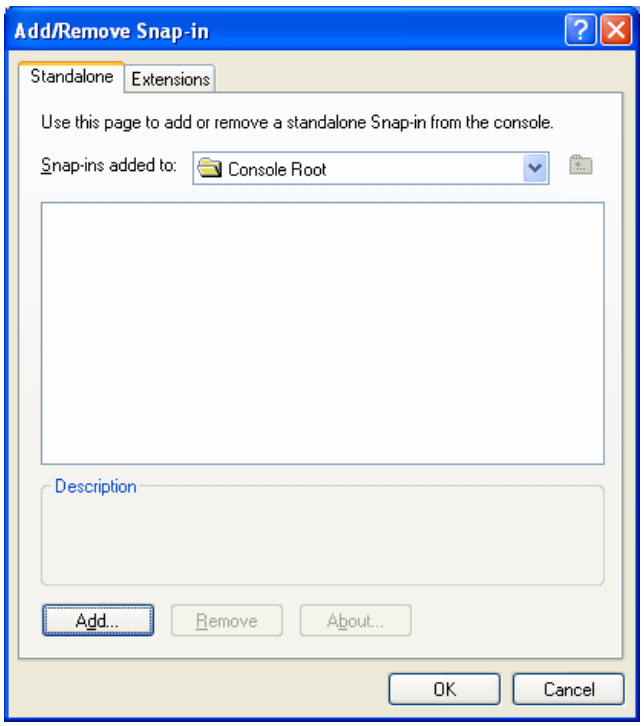
1. Open the Windows **Start** menu and select **Run**.
2. Type 'MMC' (without quotes) and click **OK**.



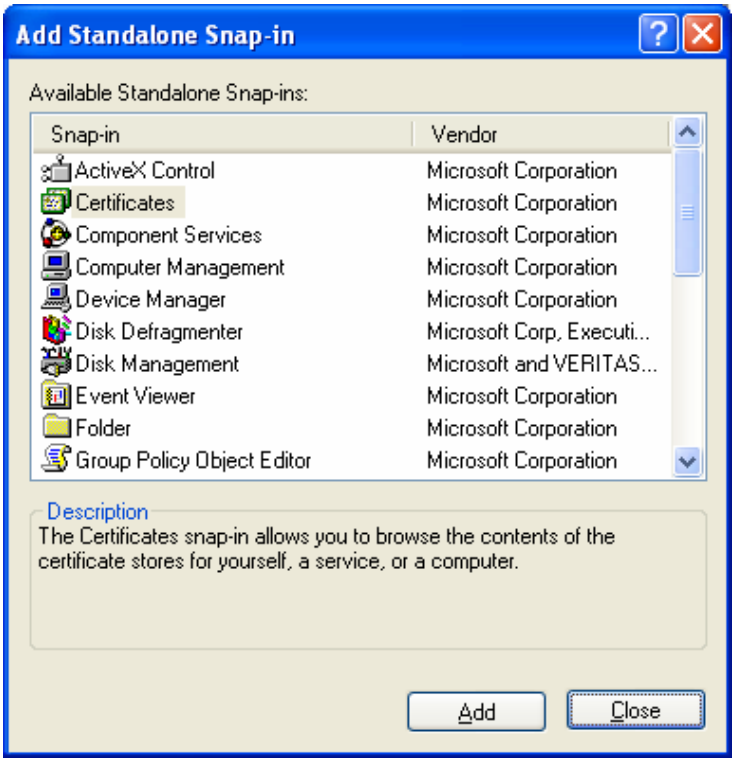
3. The MMC will open in a window titled *Console 1*.
4. Hold down the *Control* button and hit the *M* key (CTRL+M) on your keyboard. This typing will not display on the screen, but should open a new window.
   - Alternatively, you may select the **Console** menu and choose **Add/Remove Snap-in**.



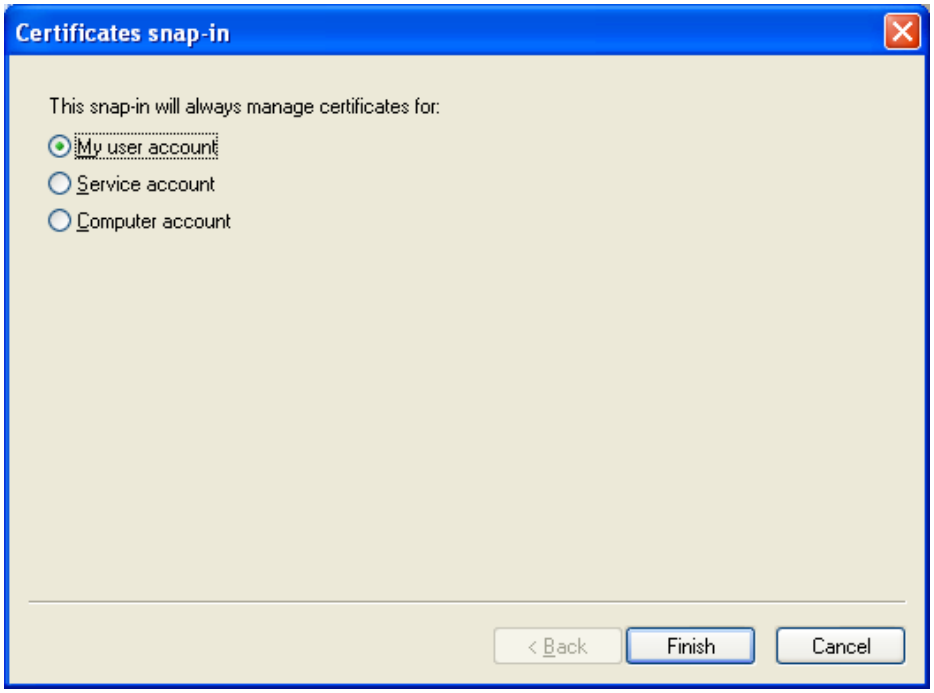
5. The *Add/Remove Snap-in* screen opens. Click the **Add** button.



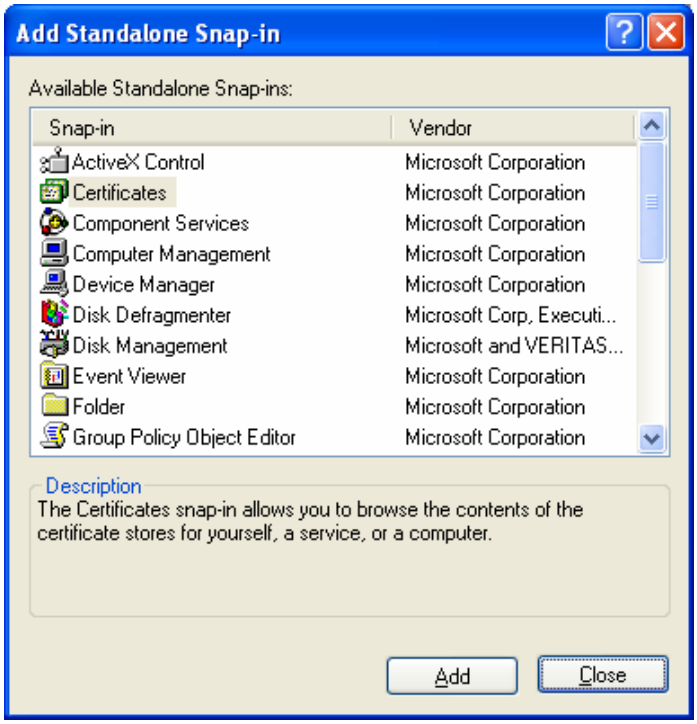
6. A new screen opens that lists *Available Standalone Snap-ins*. Select **Certificates** and click the **Add** button.
   - The Certificates snap-in is an alternate way to view the user's certificate store rather than using Internet Explorer.



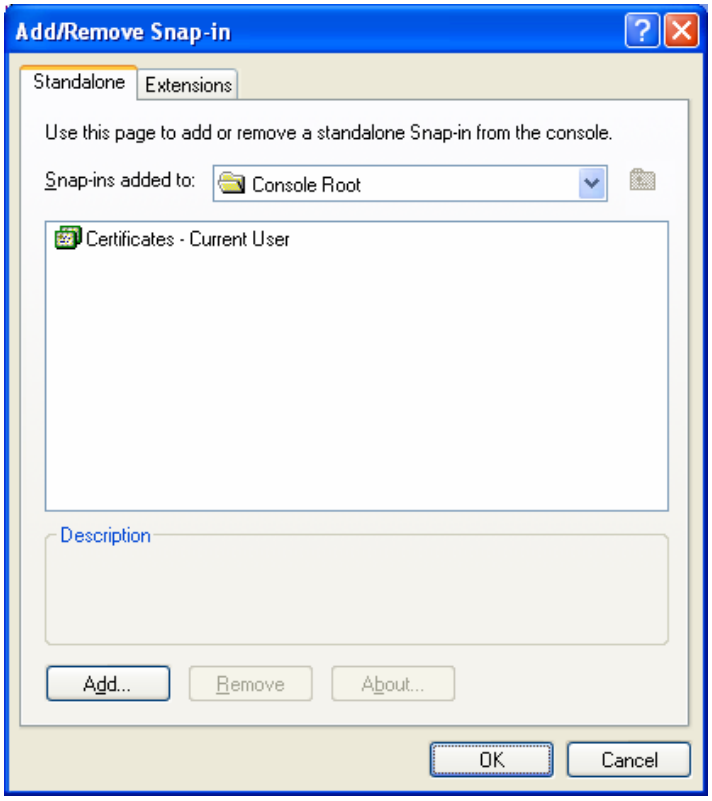
7. A *Certificates snap-in* screen opens. Select **My user account** and click the **Finish** button.



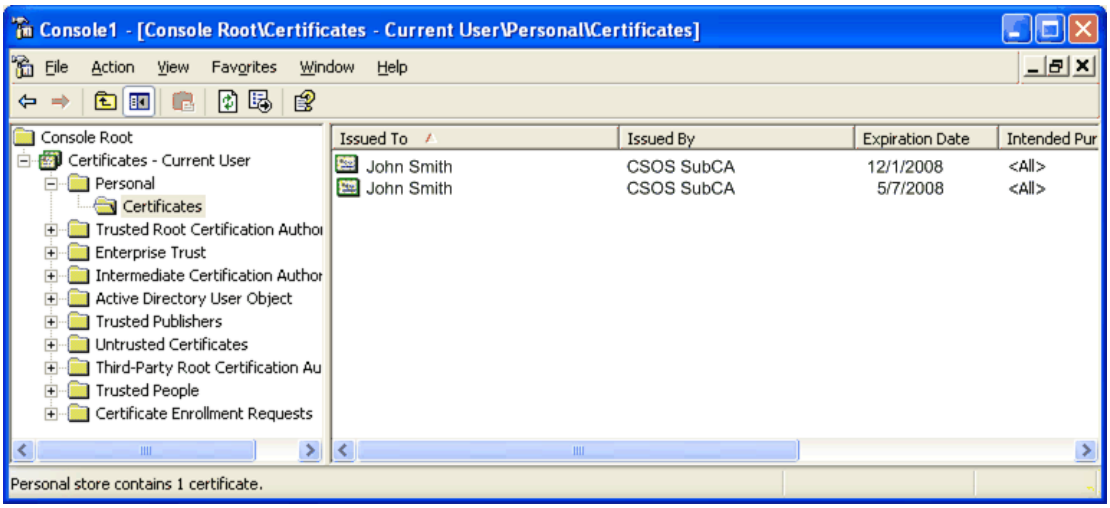
8. At the *Add Standalone Snap-in / Available Standalone Snap-ins* screen, click **Close**.



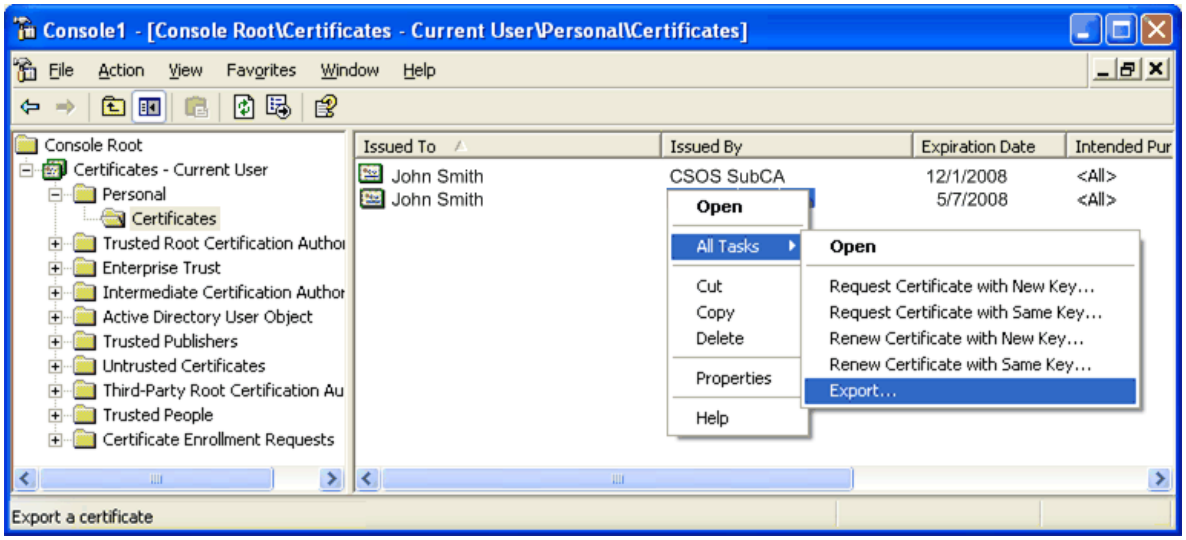
9. At the *Add/Remove Snap-in* screen click **OK**.
   - Note: *Certificates – Current User* will be displayed on this screen.



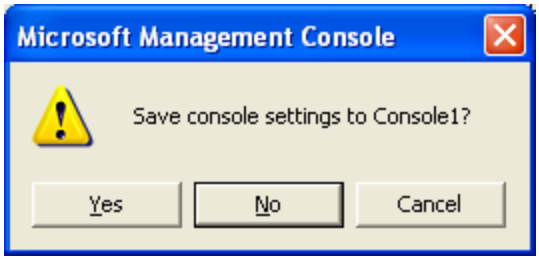
10. In the *Console Root* screen, the *Certificates – Current user* snap-in is displayed. Open this snap-in, double click on the *Personal* folder, and then open the *Certificates* folder.
    - CSOS certificates will be listed as being issued by "CSOS CA"



11. To export a certificate found in the MMC, right click on the certificate and selected **All Tasks** > **Export…**. Certificate export instructions are included in this Guide (see table of contents).



12. When closing the MMC, you will be prompted to "Save console settings to Console1?" Saving the settings is not necessary unless you plan on accessing certificates via the MMC at a future time.



Locating certificate files

A certificate may not be found in the Web browser (Internet Explorer, Netscape, Firefox) for the following reasons:

- The certificate has been removed from the certificate store.
- The certificate has been transferred from another computer and was never installed into the certificate store on the current computer.
- The certificate is installed on a token device (such as a smart card) that is not currently installed on the computer – this topic is not covered in this Guide.
- The certificate did not install successfully during the retrieval, despite a successful confirmation from the retrieval Web page.

If the certificate is not in a browser's certificate store, it may be on the hard drive in the form of a PFX or P12 file, which can be found by performing a search of the hard drive.

Searching for a file will vary depending on the version of the operating system being used.

Search using Windows XP:

1. Select the Windows **Start** button and click **Search**.
2. Select **All files and folders** if given the option of "What do you want to search for?"
3. In the *All or part of the file name:* field type "*.pfx" and click **Search**.
   - Verify that the C drive is selected in the *Look in*: field.
4. The search will locate any certificates on the computer that have been exported from the certificate store or have been transferred in from another computer.
5. Certificate files found on the computer will be displayed. These pfx certificate files may potentially be installed in the browser or ordering software certificates store. Information contained in the certificate that may be used to identify it will not be accessible until the certificate has been imported into a certificate store.

Search using Windows 2000:

1. Select the Windows **Start** button and select **Search** –> **For Files or Folders…**
2. In the *Search for files or folders named:* field type "*.pfx" and click **Search Now**.
   - Verify that the C drive is selected in the *Look in*: field.
3. The search will locate any certificates on the computer that have been exported from the certificate store or have been transferred in from another computer.
4. Certificate files found on the computer will be displayed. These PFX certificate files may potentially be installed in the browser or ordering software certificate store. Information contained in the certificate that may be used to identify it will not be accessible until the certificate has been imported into a certificate store.

Identifying CSOS Certificates

Two types of certificates are issued to CSOS subscribers. When configuring CSOS ordering software, it is important to locate the correct certificate to be used for electronic ordering.

a) **CSOS Signing Certificates** are used for digitally signing electronic orders of controlled substances. Signing Certificates are issued to Registrants, Power of Attorneys, and (if requested) to Coordinators. Each Signing Certificate is issued to an individual and is specific to one DEA Registration. Subscribers who order for more than one location require a Signing Certificate for each location. Information regarding the DEA Registration is contained in each signing certificate. This information includes:

   Registrant name

   Registrant address

   DEA Number (hashed with the Certificate Serial Number)

   Authorized Drug Schedules

   Signing Certificates are valid until the subscribers DEA Registration expires.

b) **CSOS Administrative Certificates** are used for digitally signing communications and may not be used for controlled substance ordering. A typical use of an Administrative Certificate is for digitally signing an E-mail Certificate revocation or renewal request. Administrative Certificates are issued to CSOS Coordinators and Registrants serving as Coordinator. Administrative Certificates do not contain authorized drug schedules and are not specific to a DEA Registration. Administrative Certificates are valid for three (3) years from the date of issuance.

Issuance of these certificates will vary depending on the subscriber type.

a) **Registrants** are issued one CSOS Signing Certificate for each approved DEA Registration number. Registrants serving as Coordinator will also be issued a CSOS Administrative Certificate.

b) **CSOS Coordinators** are issued one CSOS Administrative Certificate, regardless of the number of DEA Registrations for which he/she is a Coordinator. Additionally, Coordinators requesting signing authority are issued one CSOS Signing Certificate for each approved DEA Registration number.

c) **CSOS Power of Attorneys** are issued one CSOS Signing Certificate for each approved DEA Registration number.

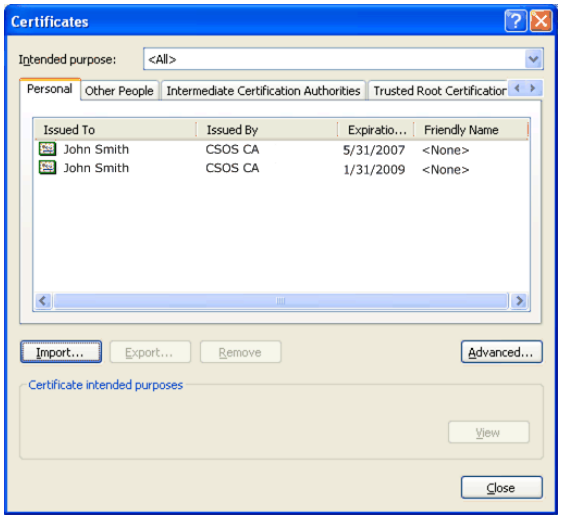
Identify certificates using the expiration date (easiest method)

⚠ Use the following identification method if only one DEA Registration number is involved or if multiple DEA Registration numbers have unique expiration dates. If using this method does not provide an obvious identification, **do not guess**; the certificate will need to be identified using a more precise method.

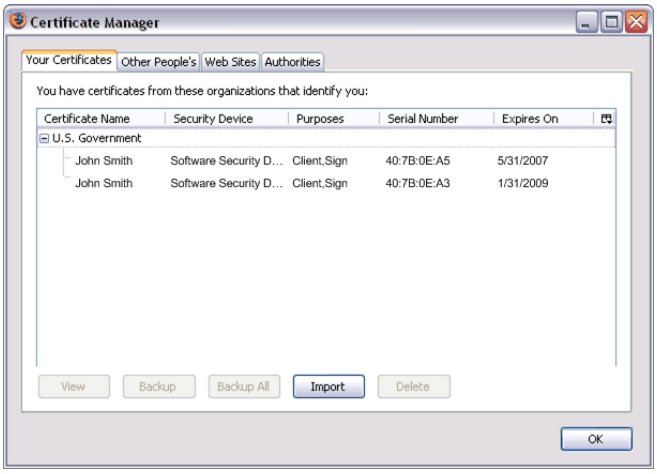
- **CSOS Signing Certificates**: expire when the associated DEA Registration expires. DEA Registrations are valid for either one (1) or three (3) years depending on the registration's business activity. If the registration expiration date is known, then the Signing Certificate is typically easy to identify. Please note, the certificate expiration date may be indicated as one day before the DEA Registration states.
- **CSOS Administrative Certificates**: expire three (3) years from the date it was issued.

In the example below, for a customer activating certificates in **February of 2006**:

- The certificate expiring 1/31/2009 would be the Administrative Certificate
- The certificate expiring 5/31/2007 would be the Signing Certificate
  - This is easily determined since the certificate is valid for *less than* three years (ruling out the possibility that it is an Administrative Certificate)



Internet Explorer Certificate Store

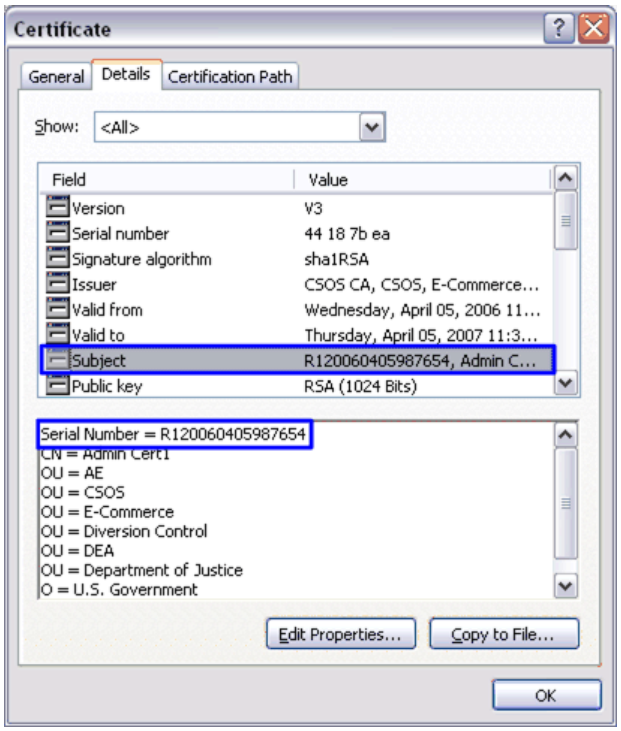


Mozilla Firefox Certificate Manager

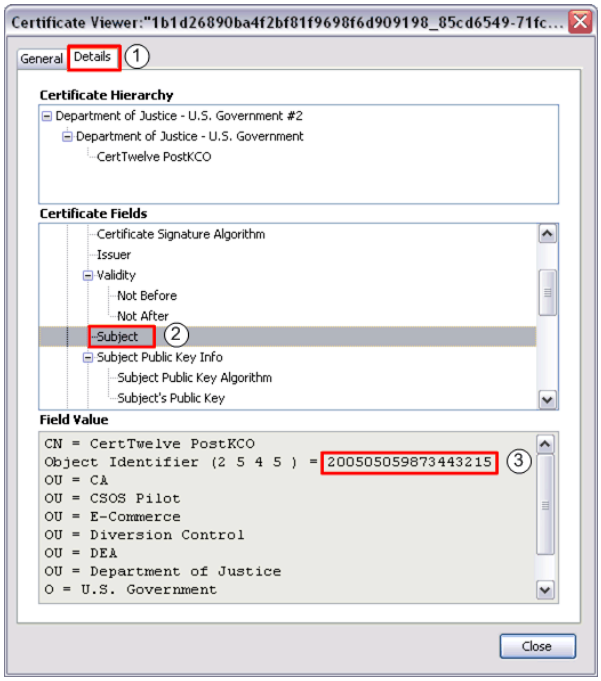
Identify using the Certificate Serial Number (more accurate method)

Each CSOS certificate has a unique serial number, which may be used to identify the certificate. The serial number is indicated on the certificate owner's postal mailed activation notice as well as in the certificate on the details tab. Identifying certificates base on the serial number may be necessary if the subscriber has certificates for multiple DEA Registration numbers or if certificates have been revoked and/or renewed.

1. With the certificate store open (see “Finding Certificates”), double click on a certificate issued by CSOS CA.
2. The *Certificate* screen opens. Select the *Details* tab and highlight the **Subject** field.



Internet Explorer



Firefox and Netscape

3. The Serial Number listed in the certificate's Subject field matches the serial number indicated on the postal mailed activation notice from DEA

IMPORTANT INFORMATION ON ACTIVATING YOUR CSOS CERTIFICATE
Combine this information with the access code you received via E-Mail for this DEA Registration Number. **Please retain this document for future management of your certificate.**

DEA Diversion E-Commerce Support
E-Mail: csossupport@DEAecom.gov
Phone: 1-877-DEA-ECOM (1-877-332-3266)

Name:	John Smith
E-Mail address:	John.Smith@Internet.com
CSOS Account Number:	0000
Certificate Serial Number:	R00002005001
CA Thumbprint (SHA-1):	FEBF F1A8 F348 4ABD A146 E64B 5760 21C7 AAAB 43AF

Step 1 – Locate your E-Mail containing this same DEA Registration Number

DEA Registration Number:	XX1234567

Step 2 – Use this information to log in to the DEA E-Commerce Certificate Retrieval Web page

Web site Address:	<Web site Address>
Web site Username:	<Web site Username>
Web site Password:	<Web site Password>

Step 3 – Use this Access Code Password, along with the Access Code from your E-Mail to activate your certificate

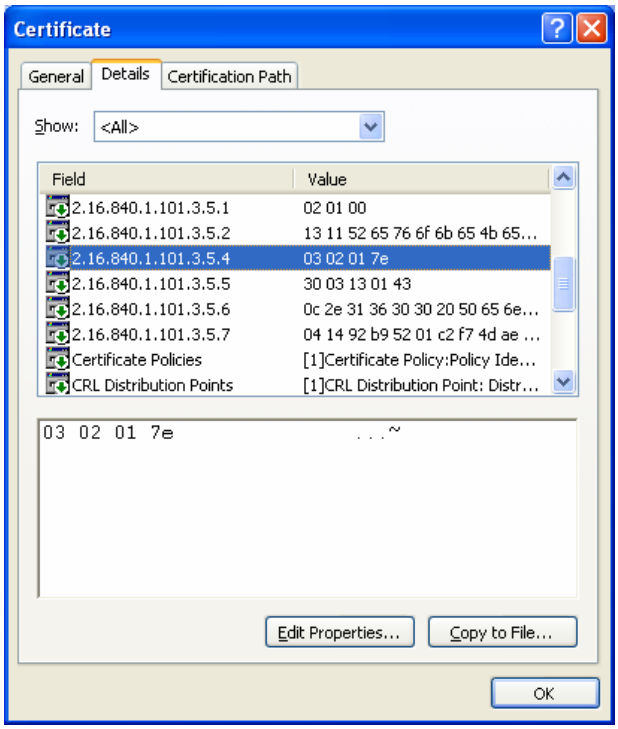
Access Code Password:	<Access Code Password>

- If this notice is not available and the certificate cannot be identified, then call DEA Diversion E-Commerce Support (1-877-332-3266) who will be able to identify the certificate.

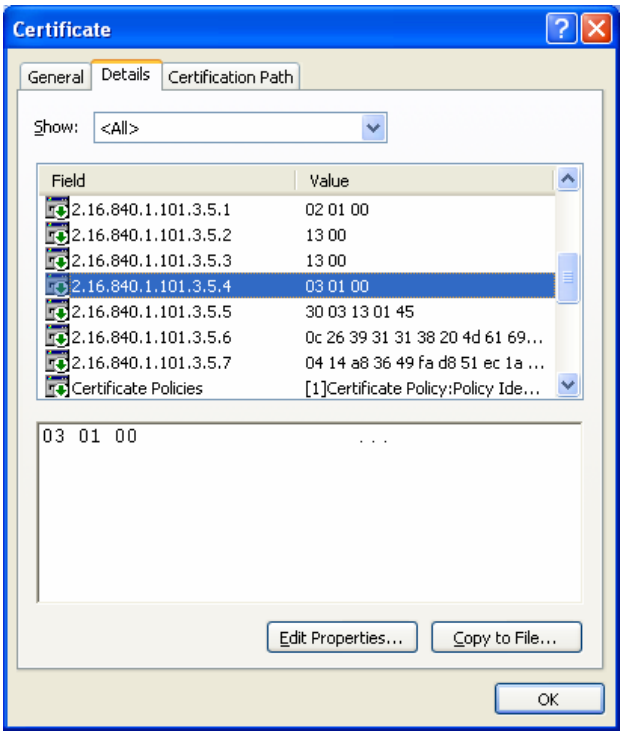
Identify certificates using valid ordering schedules (last resort method)

One last method that will only distinguish between ***one*** subscriber's administrative certificate and signing certificate (he/she must *only* have *one* signing certificate for this method) is to view what controlled substance schedules the certificate is valid for.

A CSOS Signing certificate contains an OID (Object Identifier) that indicates the controlled substance schedules (classes) the certificate is valid for. A Signing certificate valid for all schedules II-V (2, 2n, 3, 3n, 4, and 5) will include '7E' in the OID field ending in 4 as the example on the left indicates. This value will vary depending on the authorized schedules, however the majority of certificates are valid for all schedules II-V. The Administrative certificate on the right contains the value '00' in the OID field since Administrative certificates are not valid for ordering any schedules.



CSOS Signing Certificate



CSOS Administrative Certificate

Certificate Export

Introduction on Certificate Export

Certificates may only be activated once. During activation, the certificate is placed in the certificate store of the Web browser. To copy the certificate from the certificate store, the certificate must be exported. Reasons for exporting a certificate include:

1. Transferring the certificate to another computer
2. Backing up the certificate
3. Copying from the certificate store for installation in CSOS ordering software

Certificate export creates a file with a .pfx extension (.p12 for Firefox and Netscape activated certificates). If exported correctly, this exported certificate file will be a copy of the subscriber's certificate containing the associated private key (used for digital signatures). The original copy of the certificate (with private key) will remain in the browser's certificate store unless it is actively removed.

Export procedures will vary depending on the type of browser being used. Once the certificate has been located (see "Locating Certificate Files"), the following export procedures may be used to create a PFX or P12 file capable of being installed into the ordering software.

Important notes:

⚠ These procedures must be followed *exactly*. Variance from these procedures may render the certificate invalid or require revocation by DEA due to policy violation.

⚠ The owner of the certificate is required to be present for certificate export and is the only person authorized to enter the certificate's password.

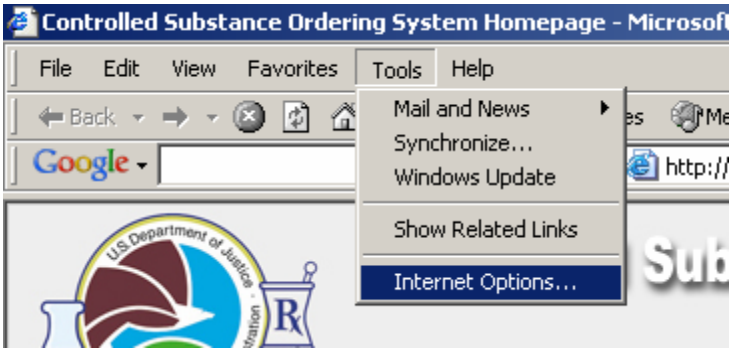
⚠ The CSOS CA encourages support representatives to **not** remove certificates from the certificate store following export. Certificates should be stored permanently in the Web browser in addition to being exported and installed into ordering software.

Certificate Export - Internet Explorer

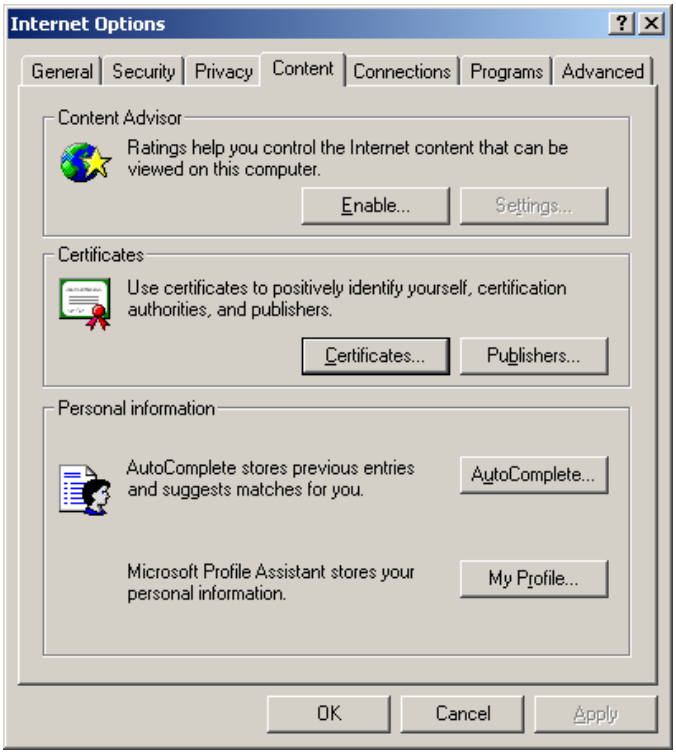
Purpose: These certificate export instructions may be used to copy a certificate from the Internet Explorer certificate store. Once the certificate has been exported it may be backed up, transferred to another computer, or imported into the certificate store of the ordering software.

⚠ **The owner of the certificate is required to be present for certificate export and is the only person authorized to enter the certificate's password**. Certificates exported without the owner present are subject to certificate revocation by DEA.

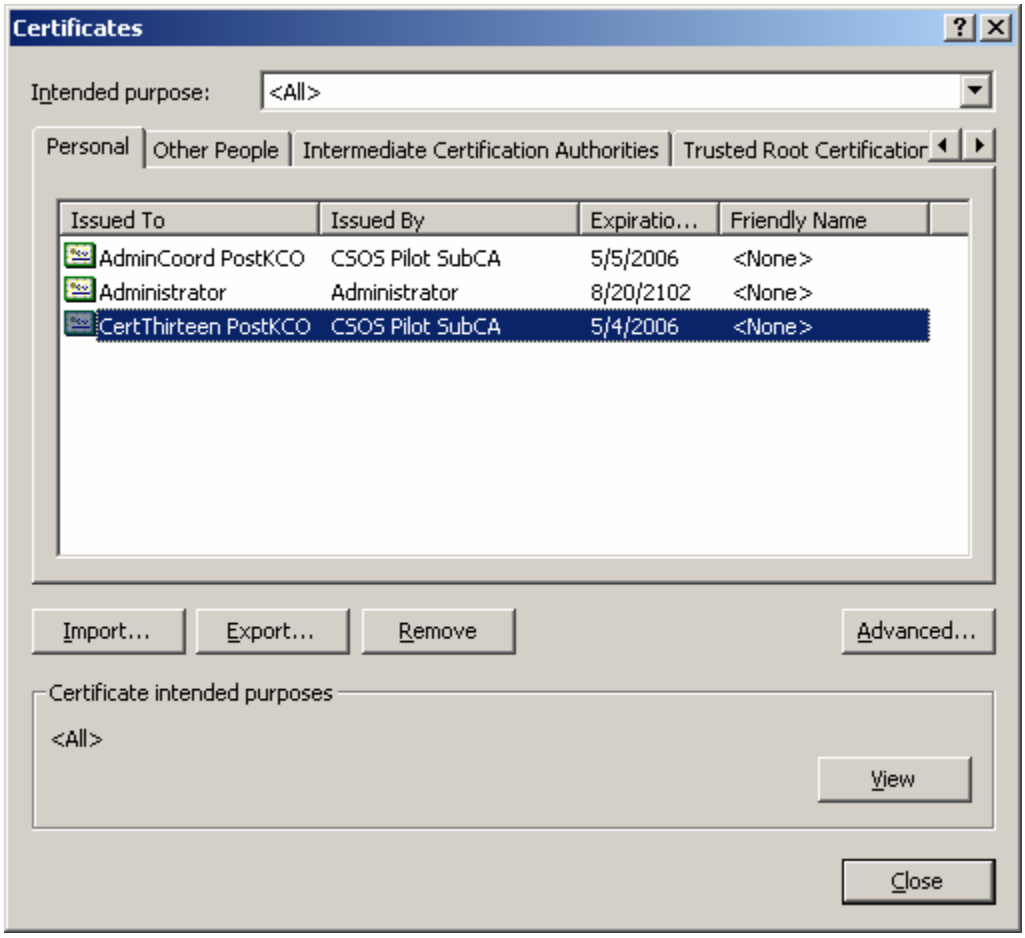
1. Open Internet Explorer.
2. Open the **Tools** menu and select **Internet Options**.



3. Switch to the **Content** tab and click the **Certificates…** button.



4. Select the CSOS Certificate to export and click the **Export** button.
   - CSOS Certificates are issued by "CSOS CA."
   - CSOS Administrative Certificates expire three (3) years from the date of issuance.
   - CSOS Signing Certificates expire when the associated DEA Registration expires.
   - For a more detailed explanation of identifying certificates, see "Identifying CSOS Certificates."



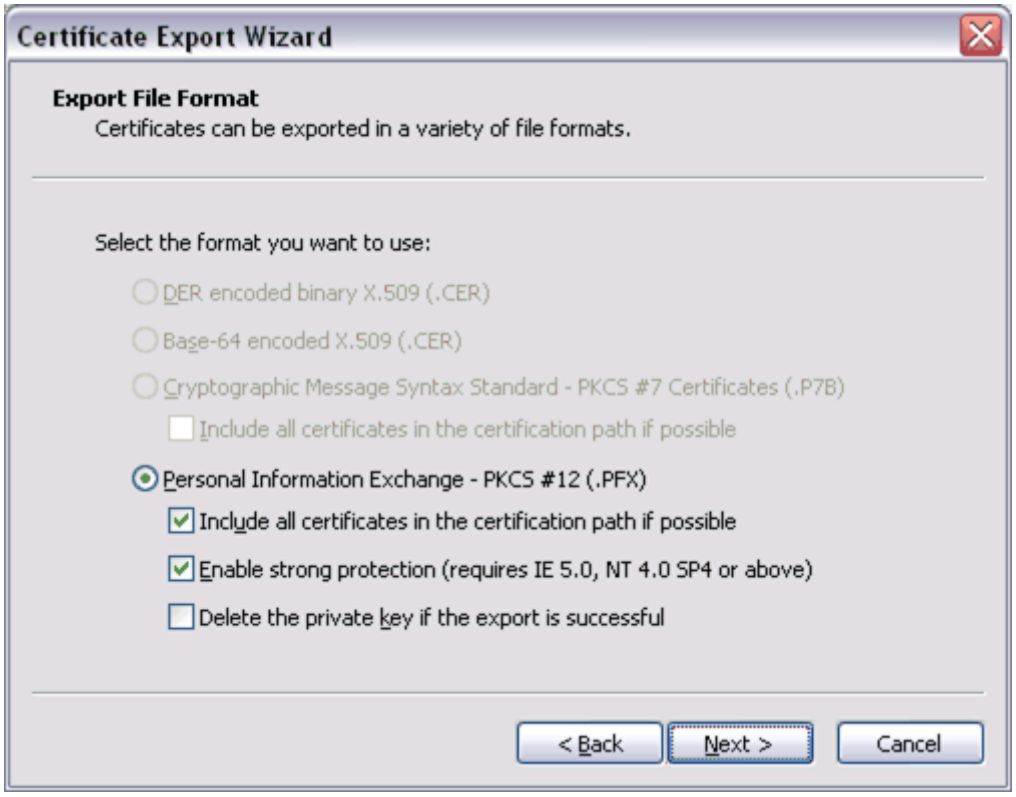
Please note: The certificate names used in this example will vary from what appears on your computer.

5. At the *Certificate Export Wizard* screen, click **Next**.

6. Verify that "**Yes, export the private key"** is selected and click **Next**.

⚠ If the "Yes, export the private key" option is not available, please contact DEA E-Commerce Support.

7. Select "Include all certificates in the certificate path if possible" and "Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)" (if not selected already) and ***only*** "Enable strong protection…" the click the **Next** button.



⚠ **Do not** select "Delete the private key if the export is successful"

Notes:

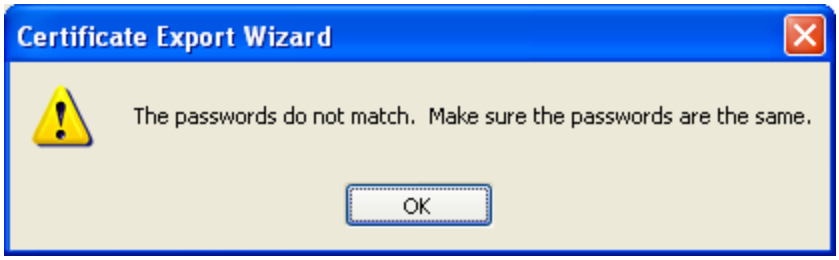
- Including all certificates in the certificate path will store the E-Commerce Root and CSOS Sub CA certificates (if found in this certificate store) with the exported PFX certificate file.
- Deleting the private key will render useless the certificate in the certificate store. If the PFX is lost, corrupted, or incorrectly exported, there will be not original certificate (with private key) to work off of.

8. Type and confirm a backup password for the certificate.

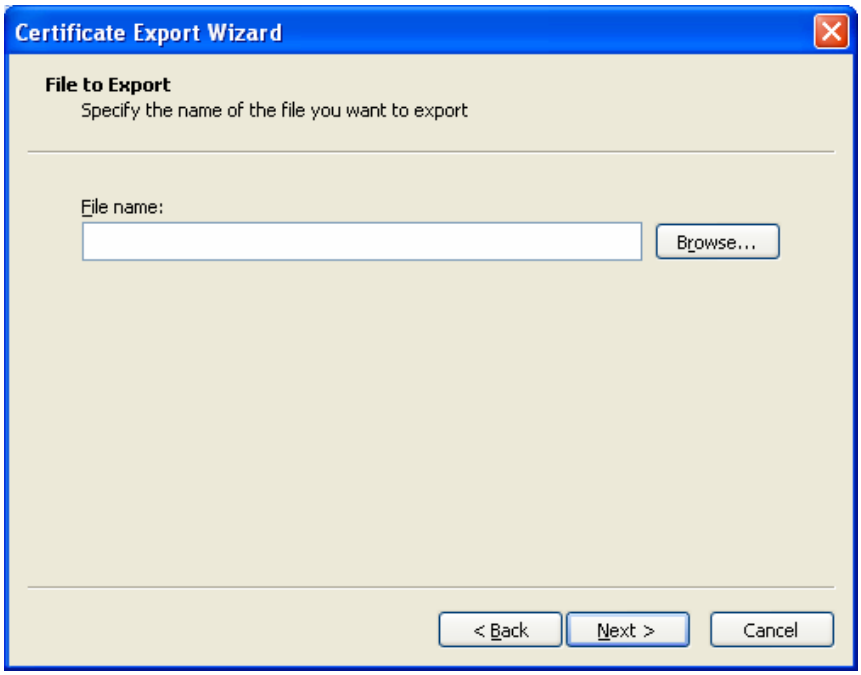
   This step allows for a backup password to be **created** for protection of the exported certificate file (PFX file). The owner of the certificate must enter this password and be the only person to know it. The password created may be the same as the certificate's private key password, which was created during retrieval.

Only the owner of the certificate may enter and have knowledge of this password.

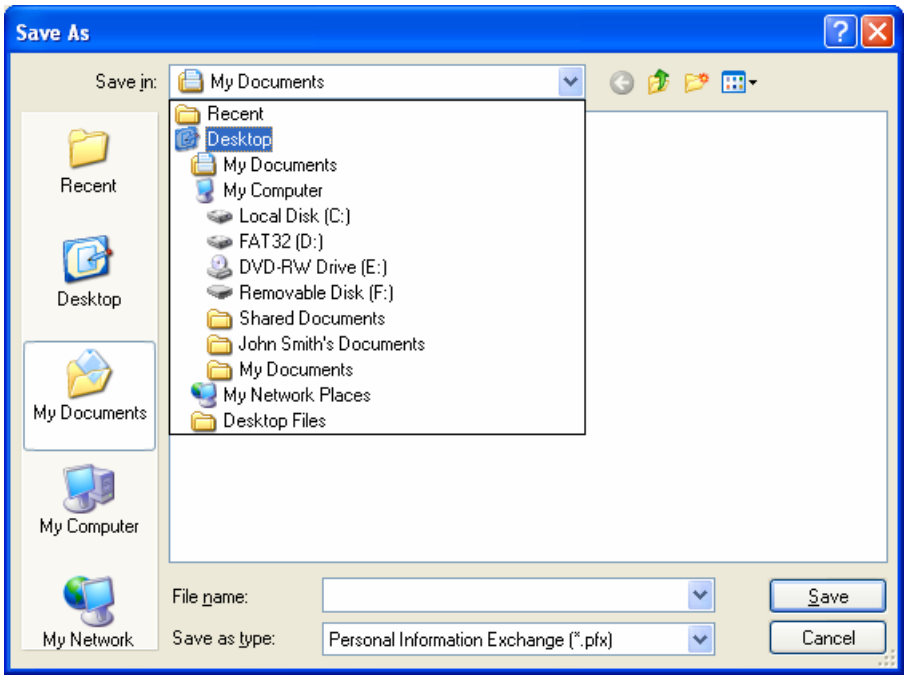
The following error will be received if the typed *Confirm password* text does not match the password.



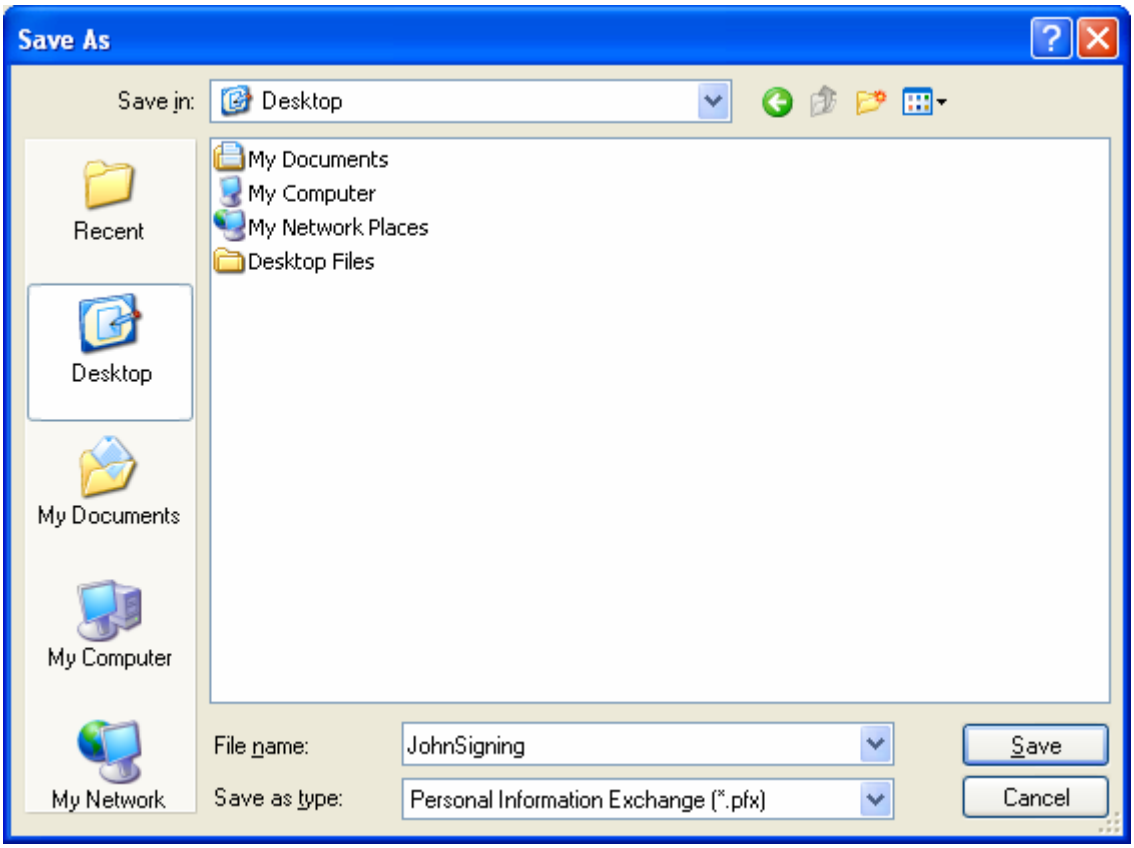
9. At the *File to Export* screen, click **Browse**.



10. Select a location to export the file to.
    - To save the file to the desktop, switch the 'Save in' drop down list to **Desktop**.
    - The certificate may be exported to a different location, but if transferring the certificate to another computer, exporting to the Desktop first is recommended.

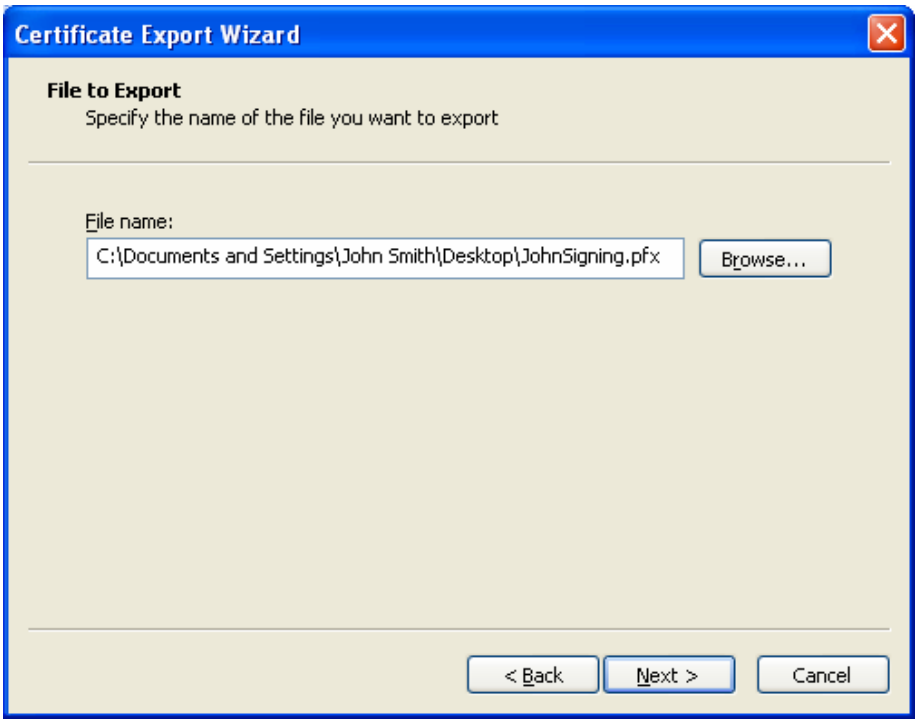


11. Enter a name for the Certificate file in the 'File name:' field and click **Save**. Naming the certificate is *very* important for identification purposes since the data in the certificate will not be visible when the certificate is in the form of a PFX file. For this reason, certificates with vague names are difficult to manage.
    - Signing Certificates should be named using one of the following naming conventions:
        - CSOSOrdering or JohnOrdering
        - CSOSSigning or JohnSigning
        - John_AB1234567 (please use when the subscriber has multiple certificates for multiple DEA Registration numbers)
    - Administrative Certificates should be named using one of the following naming conventions:
        - CSOSAdmin or JohnAdmin



12. Verify that the 'Save as type' option is set to "Personal Information Exchange (*.pfx)". Click **Save**.

13. Back at the *File to Export* screen, click **Next**.



14. At the *Completing the Certificate Export Wizard* screen, click **Finish**.

15. The *Exporting your private exchange key!* screen will vary depending on whether the certificate has a private key password or not. If there is no private key password on the certificate, simply click **OK**. If there is a password, the certificate owner will be required to enter it here before clicking **OK**.

    Do not select the *Remember password* option check box.

    Only the owner of the certificate is authorized to enter and have knowledge of this password.

16. At the *The export was successful* screen, click **OK**.

If the following error (or a similar one) is received, then the private key password was not entered correctly. Remember, this password is case sensitive and was set during initial retrieval.

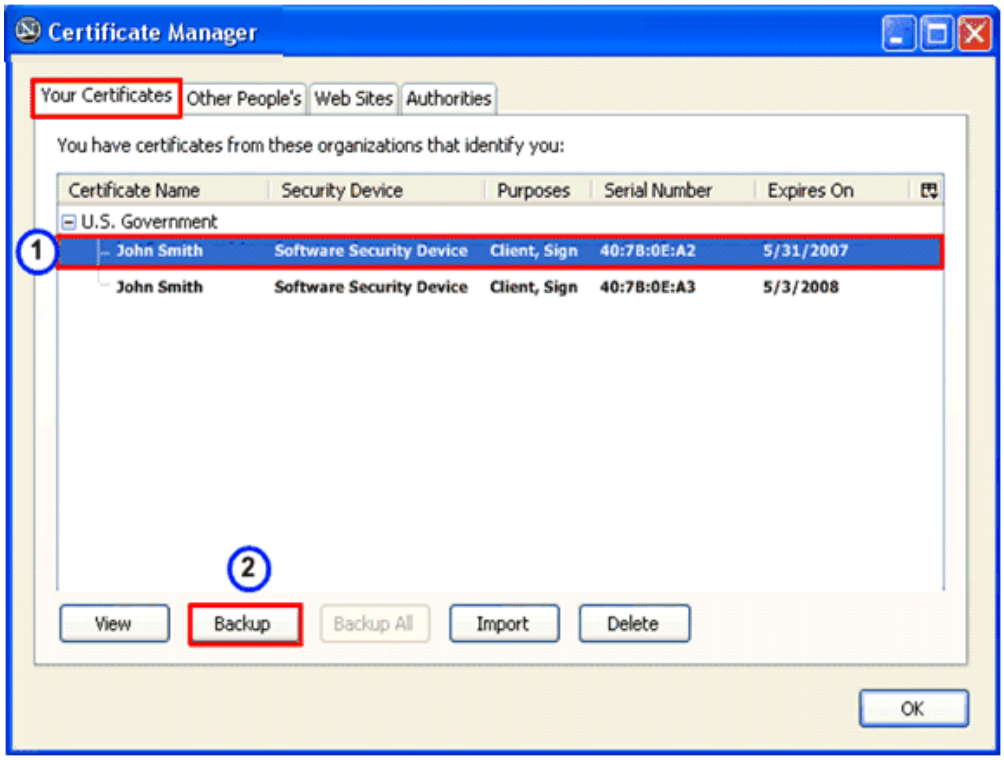
Certificate Export – Netscape

Platform: The following documentation was tested on Netscape versions 7.2 and 8.0.

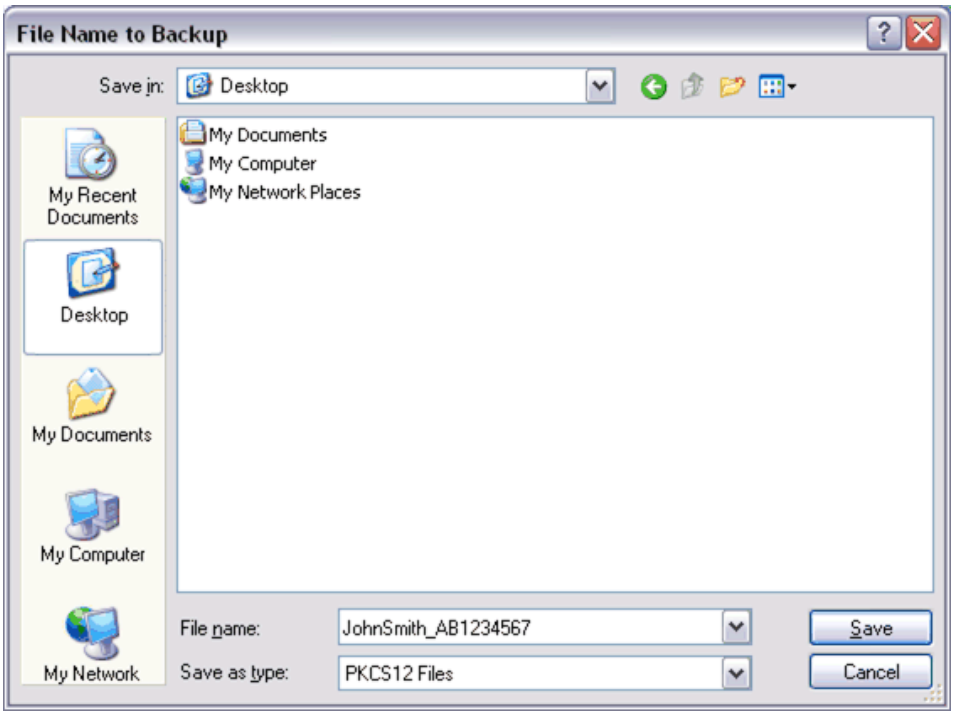
Purpose: These certificate export instructions may be used to copy a certificate from the Netscape Certificate Manager. Once the certificate has been exported it may be backed up, transferred to another computer, or imported into the certificate store of the ordering software.

The owner of the certificate is required to be present for certificate export and is the only person authorized to enter the certificate's password. Certificates exported without the owner present are subject to certificate revocation by DEA.

1. Locate the CSOS Certificate to be exported (see section "Finding Certificates"). The steps for accessing the Certificate Manager vary by Netscape version.
2. Select the CSOS Certificate (1) to export and click the **Backup** button (2).
   - CSOS Certificates are issued by "CSOS CA."
   - CSOS Administrative Certificates expire three (3) years from the date of issuance.
   - CSOS Signing Certificates expire when the associated DEA Registration expires.
   - For a more detailed explanation of identifying certificates, see "Identifying CSOS Certificates."



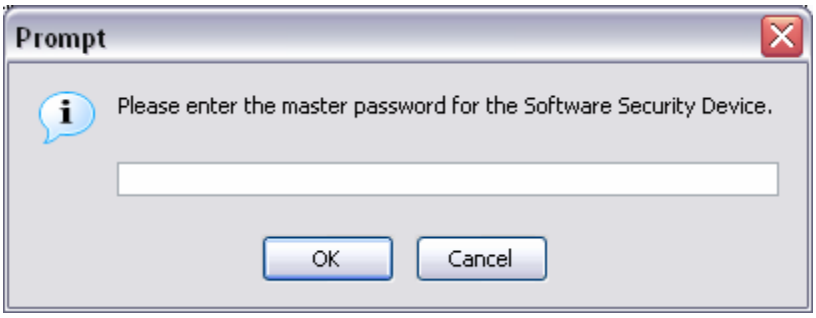
3. Set the backup location by changing the *Save in* dropdown list to Desktop. Enter a name for the Certificate file in the 'File name:' field and click **Save**. Naming the certificate is *very* important because the data in the certificate will not be visible when the certificate is in the form of a PFX file. For this reason, certificates with vague names are difficult to manage.
   - Signing Certificates should be named using one of the following naming conventions:
     - CSOSOrdering or JohnOrdering
     - CSOSSigning or JohnSigning
     - John_AB1234567 (please use when the subscriber has multiple certificates for multiple DEA Registration numbers)
   - Administrative Certificates should be named using one of the following naming conventions:
     - CSOSAdmin or JohnAdmin



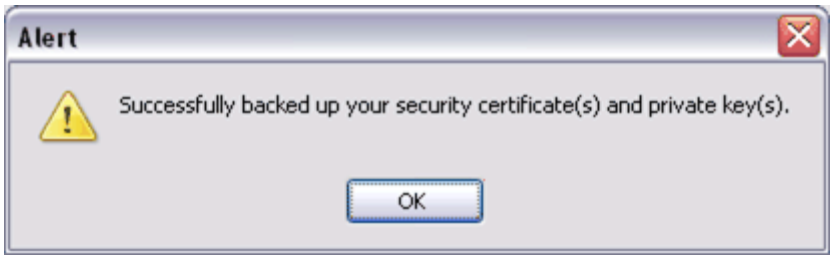
4. Type and confirm a backup password for the certificate.

   This step allows for a backup password to be **created** for protection of the exported certificate file (P12 file). The owner of the certificate must enter this password and be the only person to know it. The backup password created may be the same as the certificate's private key password, which was created during retrieval.

5. Netscape has a master password used to protect each security device, including access to certificates. This password is typically set during certificate retrieval by the customer and is not supplied or known by DEA. If this password cannot be determined, the certificate will not be accessible and a new one will need to be issued.



6. The following screen will be displayed to indicate that the certificate has been successfully backed up to a P12 file.



Certificate Export – Mozilla Firefox

Platform: The following documentation was tested on Firefox versions 1.0 and 1.5.

Purpose: These certificate export instructions may be used to copy a certificate from the Firefox Certificate Manager. Once the certificate has been exported it may be backed up, transferred to another computer, or imported into the certificate store of the ordering software.

⚠ **The owner of the certificate is required to be present for certificate export and is the only person authorized to enter the certificate's password**. Certificates exported without the owner present are subject to certificate revocation by DEA.

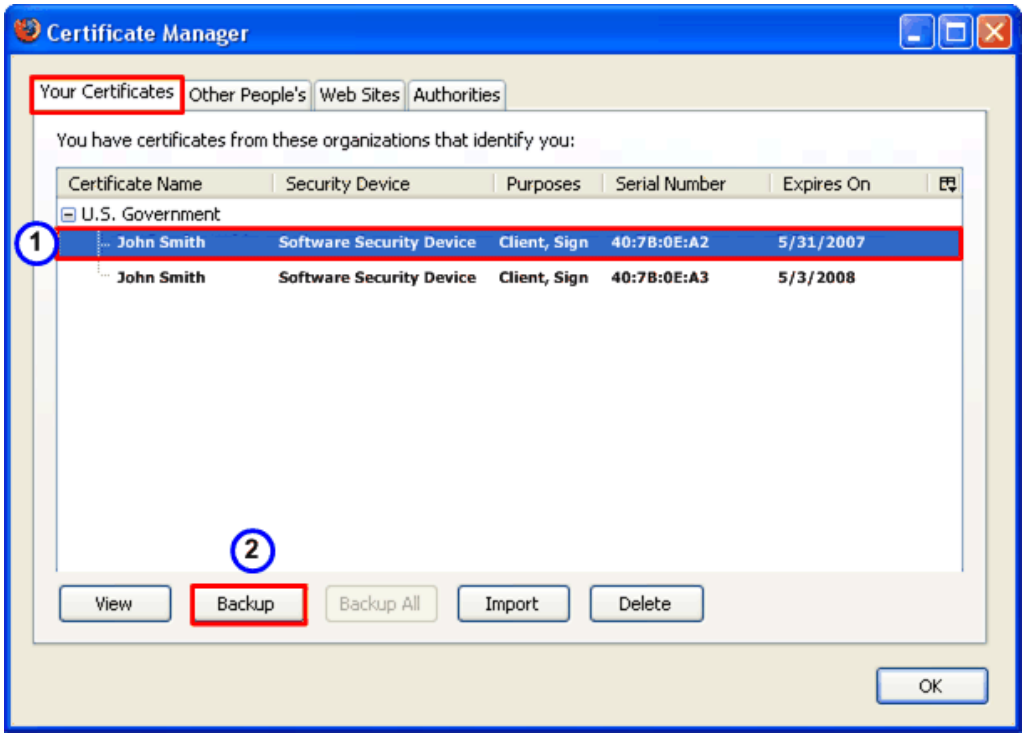
1. Locate the CSOS Certificate to be exported (see section "Finding Certificates"). The steps for accessing the Certificate Manager vary by Firefox version.
2. Select the CSOS Certificate (1) to export and click the **Backup** button (2).

   CSOS Certificates are issued by "CSOS CA."

   CSOS Administrative Certificates expire three (3) years from the date of issuance.

   CSOS Signing Certificates expire when the associated DEA Registration expires.

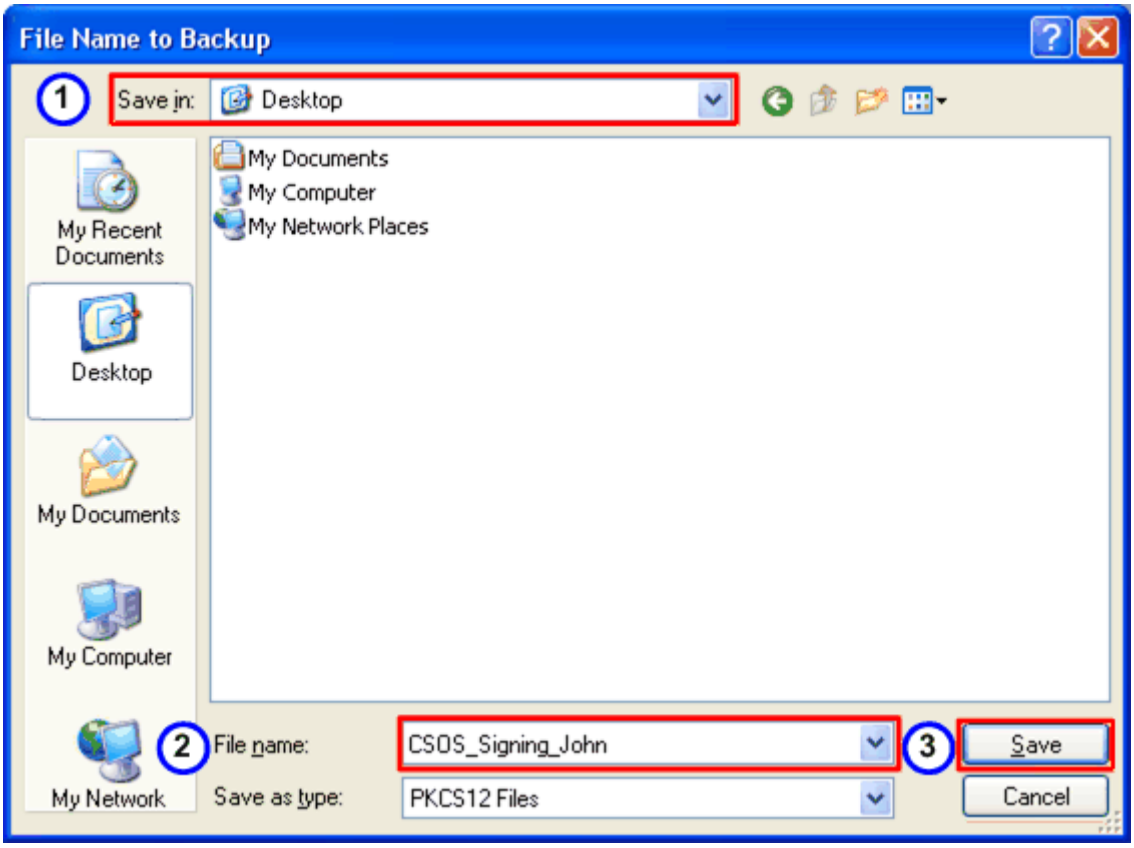
   For a more detailed explanation of identifying certificates, see "Identifying CSOS Certificates."



3. Set the backup location by changing the *Save in* dropdown list to Desktop (1). Enter a name for the Certificate file in the 'File name:' field (2) and click **Save** (3).

   Naming the certificate is *very* important for identification purposes since the data in the certificate will not be visible when the certificate is in the form of a P12 file. For this reason, certificates with vague names are difficult to manage.

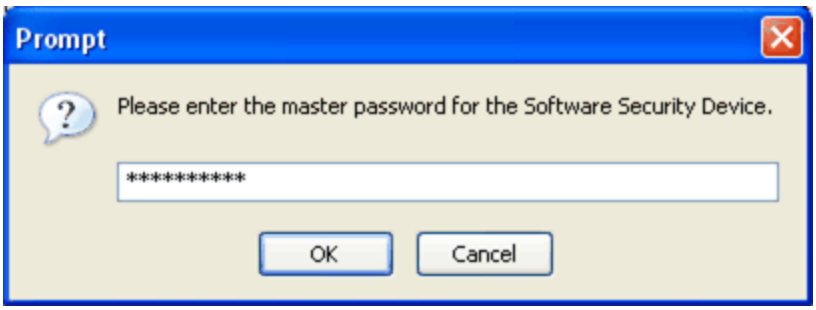
   - Signing Certificates should be named using one of the following naming conventions:
     - CSOSOrdering or JohnOrdering
     - CSOSSigning or JohnSigning
     - John_AB1234567 (please use when the subscriber has multiple certificates for multiple DEA Registration numbers)
   - Administrative Certificates should be named using one of the following naming conventions:
     - CSOSAdmin or JohnAdmin



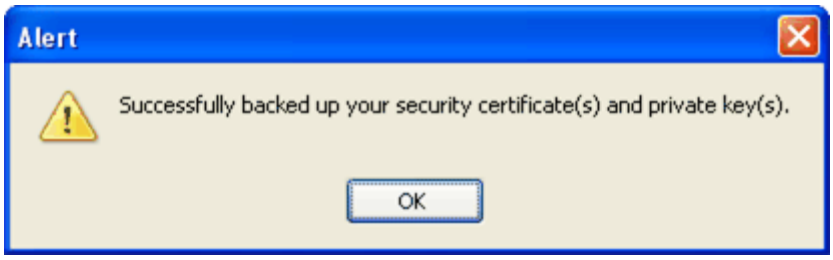
4. Type and confirm a backup password for the certificate.

   This step allows for a backup password to be ***created*** for protection of the exported certificate file (P12 file). The owner of the certificate must enter this password and be the only person to know it. The password created may be the same as the certificate's private key password, which was created during retrieval.

5. Firefox may have a master password used to protect each security device, including access to certificates. This password is typically set during certificate retrieval by the customer and is not supplied or known by DEA. If this password cannot be determined, the certificate will not be accessible and a new one will need to be issued.



6. The following screen will be displayed to indicate that the certificate has been successfully backed up to a P12 file.



Certificate Import

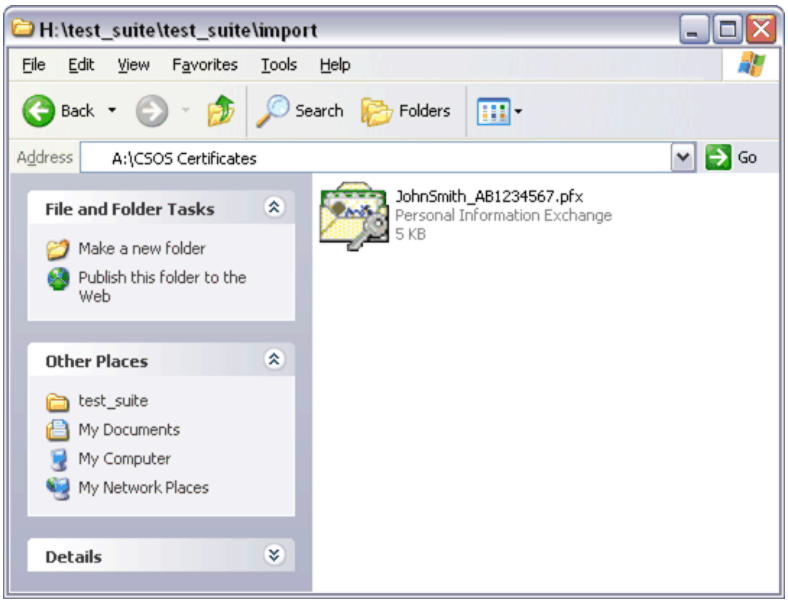
Certificate Import – Internet Explorer

Exporting a certificate from Internet Explorer creates a PFX file of the certificate. This file may be transferred or backed up just like any other file. These certificate import procedures should be used to install a PFX file into an Internet Explorer certificate store.

Use these certificate import procedures to:

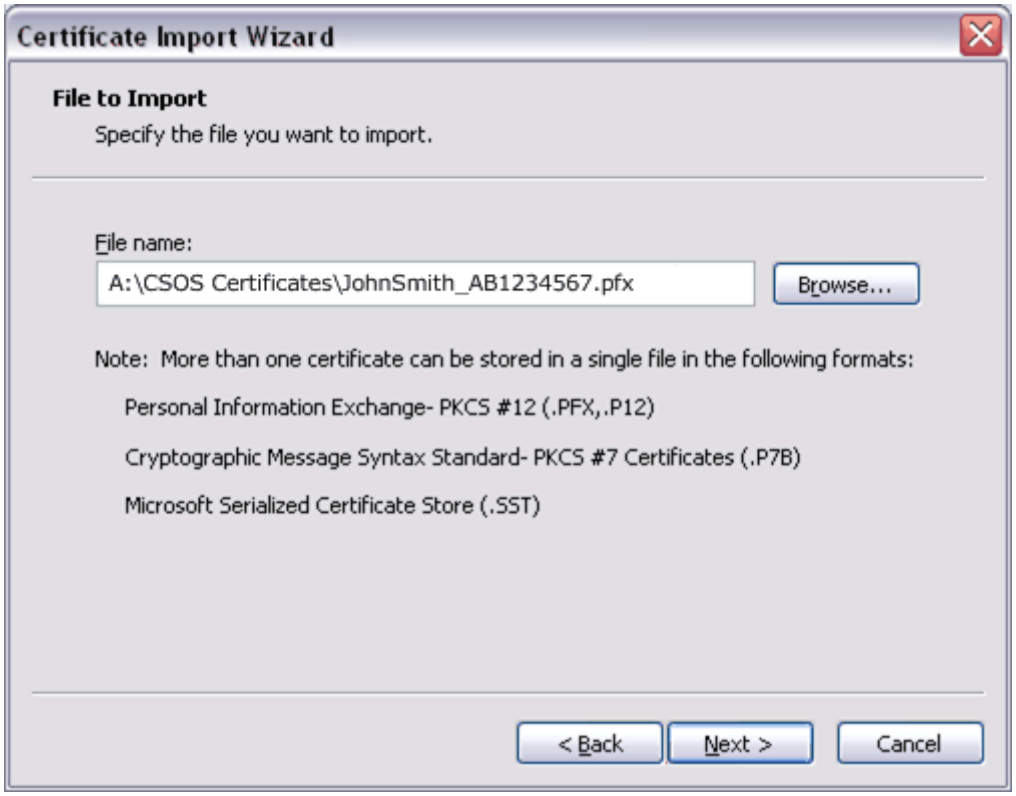
- Install a previously exported CSOS Certificate on a new computer.
- Install a CSOS Certificate that has been backed up (i.e. restore from floppy disk backup after a hard drive crash).
- Install a previously exported CSOS Certificate for the purpose of setting a new private key password (see "Certificate Transfer").

1. Locate the PFX file and double click on it.



2. The *Certificate Import Wizard* opens. Click **Next**.

3. At the *File to Import* screen, click **Next**.



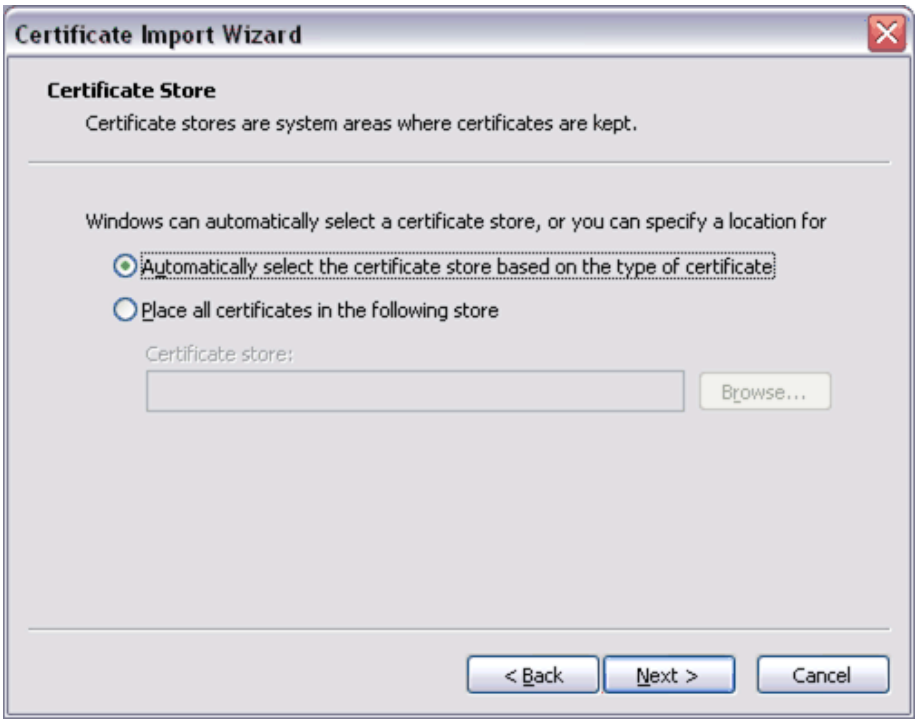
4. Enter the certificate's backup password. This is the password created when the PFX certificate file was exported. If no backup password was set, leave this password field blank.

   Select ***both*** checkboxes to "Enable strong private key protection…" and "Mark this key as exportable…"

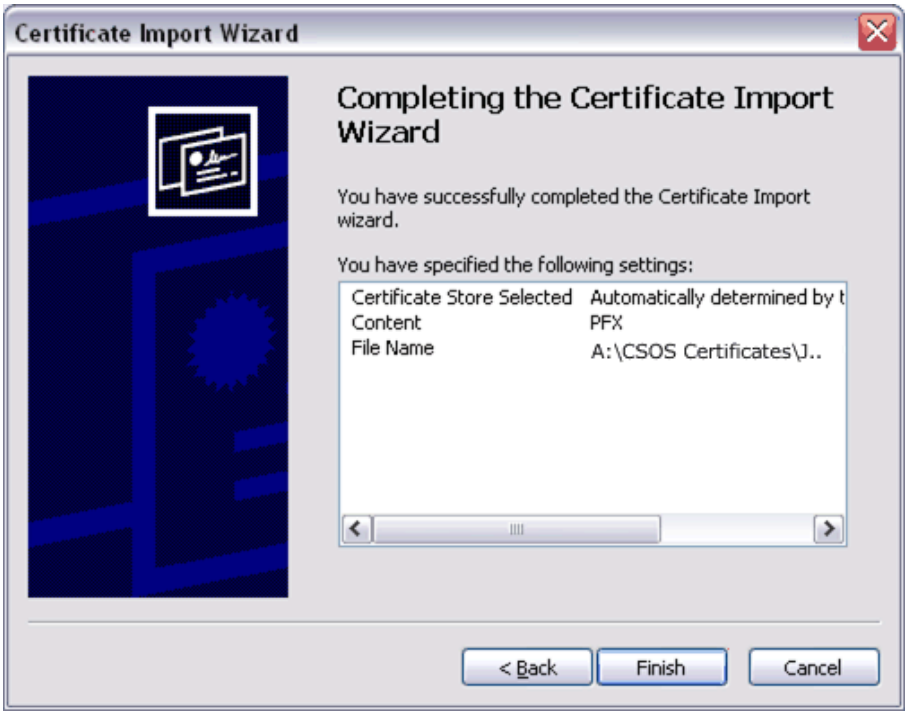
   ⚠ Not selecting both checkboxes will result in an unsecured and typically unusable (for ordering purposes) certificate.

If the backup password was not entered correctly, the following prompt is displayed. Click **OK** and attempt to enter the correct backup password again. Remember that a backup password may not have been set, in which case the *Password* field should be left blank.

5. Verify that *Automatically select the certificate store…* is selected and click the **Next** button.



6. Click the **Finish** button.



7. The next steps allow for a private key password to be set. A private key password is a policy requirement and is essential in protecting the digital certificate. Click the **Set Security Level** button.

8. Set the security level to **High** and click the **Next** button.

9. Create the private key password.

This information is to be entered and known by the owner of the certificate only! The owner of the certificate is the *individual* whose name appears on the inside of the postal mailed activation notice for this certificate. Knowledge of this password by any party other than the certificate owner, including a co-worker, spouse, or support representative, constitutes a private key compromise and the certificate is subject to revocation by DEA.

- Enter the name of the certificate owner in the **Password for** field.
  - The name does not need to be entered in any specific format
  - This field is often grayed out and no information may be entered. This is OK.
- Enter a password in the **Password** and **Confirm** fields.
  - The customer must remember this password and do not share it with anyone
  - If this password is forgotten, lost, or compromised a new certificate must be issued. Please stress this issue if working with a customer
  - This password is CaSe SeNsItIvE, therefore the customer must be aware of any capitalization used when creating the password.
- When all fields are complete, click **Finish**.

10. Click the **OK** button to continue. Note that the security level is now set to "High".

11. The following prompt indicates successful certificate import. Click the **OK** button. The certificate is now installed in the Internet Explorer certificate store for this computer. The private key password will be required any time this certificate is used.

Certificate Transfer

Once exported/backed-up, certificates may be transferred just like any other file on a computer. Certificate transfer is useful when a certificate needs to be installed for ordering on a different computer than the computer used for retrieval.

⚠ During transfer, the certificate's password will be required when accessing the certificate and a new password will be created when installing the certificate, so it is very important that the owner of the certificate is present for the transfer and is the only person controlling those passwords.

1. Export (from Internet Explorer) or Backup (from Netscape or Firefox) the certificate(s) to be transferred (see "Certificate Export"). The certificate should be exported to the Desktop of the computer unless otherwise instructed.
2. The exported/backed-up certificate file (either PFX or P12) should then be moved to the transfer media. Methods for certificate transfer include:
   - Floppy disk
   - CD/DVD
   - USB memory stick (a.k.a. "thumb drive" or "key drive")
   - Network – via a shared network drive (permissible only if the certificate's private key is protected by a password (i.e. a backup password is set).
   - E-mail – least preferable and only permissible if the certificate's private key is protected by a password (i.e. a backup password is set). ⚠ Always delete the E-mail once the certificate has been transferred.
3. Install the certificate on the new system in the browser's certificate store and/or the controlled substance ordering software's store (see "Certificate Import").
4. Once installed, all extra copies of the certificate file (PFX or P12) should be destroyed or secured.

   Certificates transferred via writable media (i.e. floppy disk, CD/DVD, memory stick) should be deleted, destroyed, or stored as backup in a secure location (i.e. safe).

   Certificates transferred via shared network drive or E-mail should be deleted once installed in a certificate store. Organizations may store password-protected certificates on shared network drives only if the computer/server is owned and managed by the registrant location or registrant's organization and proper access controls are implemented on the shared drive.

Private Key Password Reset

These instructions pertain only to certificates being managed by Internet Explorer, as Netscape and Firefox do not use certificate-specific private key passwords.

A private key password may only be set when installing a certificate into a certificate store. This password is initially set during retrieval. The following procedures may be used to set or re-set a private key password ***after*** the certificate has been retrieved.

The following steps may be used to:

- Create a private key password for a certificate that does not currently have one.
- Change an existing private key password for a given certificate.

The following steps cannot resolve forgotten passwords:

- Forgotten passwords may not be recovered. Should a password be forgotten, the certificate will require revocation by the CSOS CA and a new certificate may be issued to the subscriber.

⚠ To ensure the integrity of the DEA E-Commerce PKI system, private key passwords must not be shared. Should a party other than the subscriber acquire access to the private key password, or to a certificate that is not private key password protected, the certificate must be revoked by the CSOS CA due to key compromise.

Instructions:

1. Export the certificate from the Internet Explorer certificate store (see "Certificate Export – Internet Explorer").
    a. Create a backup password for the certificate during these certificate export steps.
    b. If the certificate does not have a private key password, there will not be a prompt to enter one on the last step.
    c. If the certificate has a private key password, the certificate owner is required to enter it on the last step.
2. Locate the exported PFX file and import it back into the Internet Explorer certificate store (see "Certificate Import – Internet Explorer").
    a. When importing the certificate, the backup password created during the export must be entered by the certificate owner.
    b. The Import instructions explain how to set the certificate's security level to high. Doing so allows for a new private key password to be created for the certificate.
3. Delete the exported PFX file and empty the Windows Recycle Bin after the certificate has been successfully imported.

4. The certificate in the Internet Explorer certificate store will be protected by the new private key password. This password will be required whenever this certificate is accessed.

4. Terminology

Activation	Synonymous with Retrieval; The process downloading a CSOS Certificate from the DEA E-Commerce Web site. Technically, this process creates a digital certificate's public and private key pairs, notifies the CA of the public key, and installs the certificate in the client's Web browser.
Applicant	An individual applying for, but not yet issued, a CSOS digital certificate.
Approved Schedules	Each DEA Registration is approved for ordering a specific set of controlled substance schedules. CSOS certificates include these approved schedules in an OID field.
ARL	See Authority Revocation List.
Authority Revocation List	A listing of revoked (invalidated) Certification Authority certificates. In the CSOS framework, the E-Commerce Root CA publishes and signs this public list, which would indicate whether any CSOS Sub CA certificate has been revoked.
Backup	The process of creating a P12 Certificate file from a certificate in a Netscape or Firefox Certificate Manager.
Backup Password	A password created during export/backup to protect the PFX/P12 certificate file. Any access to this certificate file will require knowledge of the backup password.
CA	Certification Authority; A trusted third-party that issues digital certificates and attests for the validity of each certificate issued.
Certificate	See Digital Certificate.
Certificate Manager	The utility within Netscape and Firefox that allows access to certificates retrieved and/or installed using that browser. Within the certificate manager, certificates may be viewed, backed up, or imported.
Certificate Revocation List	A listing of revoked (invalidated) certificates. The CSOS CA publishes multiple CRL(s) of all revoked CSOS certificates, which suppliers must verify before authorizing each CSOS transaction.
Certificate Store	The certificate storage location on a computer. Internet Explorer, Netscape, and Firefox provide access to certificates that have been retrieved and/or installed using that browser. This logical access location is referred to as the browser's certificate store throughout this Guide. Specifically to Windows and Internet Explorer, there are several certificate stores. CSOS subscriber certificates (both Signing and Administrative) are held in the Personal store. The CSOS Sub CA certificate is held in the Intermediate Certification Authorities store. The DEA E-Commerce Root CA certificate is held in the Trusted Root Certificate Authorities store.
Controlled Substance Ordering System	DEA's framework allowing for electronic ordering of Schedule I and II controlled substances without the requirement for a paper form DEA-222. For more information, please reference www.DEAecom.gov/about.html
CRL	See Certificate Revocation List.
CSOS	See Controlled Substance Ordering System.
CSOS Subordinate CA	DEA's certification authority (CA) for signing CSOS Subscriber Certificates and the Certificate Revocation Lists (CRLs).
CSOS Transaction	An electronic controlled substance ordering that has been digitally signed with the purchaser's CSOS certificate and placed using CSOS enabled ordering software.

Digital Certificate	A digital identity used to "sign" electronic communications including E-mails and controlled substance orders. CSOS Subscriber certificates bind publicly known information with a secret key to prove that a communication came from an authorized individual and to prevent that individual from being able to deny having digitally signed that communication.
E-Commerce Root CA	The certificate authority at the top of the certificate chain or PKI hierarchy. DEA's E-Commerce Root CA has a "self-signed", or self issued, certificate that is used to sign CSOS Sub CA certificates and the Authority Revocation List (ARL).
Enrollment	The process of requesting and being approved for a CSOS digital certificate.
Export	The process of creating a PFX Certificate file from a certificate in an Internet Explorer certificate store.
Import	The process of installing a PFX or P12 Certificate file into a Web browser certificate store.
Internet Explorer	A Web browser developed by Microsoft that is supported by the DEA E-Commerce program. Internet Explorer is available for download from www.microsoft.com.
Master Password	A password in Netscape that protects access to data stored within the browser. This password is typically created by the user during the first certificate retrieval, and is then required for all subsequent retrievals and any time a certificate is accessed (i.e. during a certificate backup).
Microsoft Management Console (MMC)	A utility in the Windows operating system that, among other services, provides access (an interface) to digital certificates installed on that computer and allows for certificate management (importing, exporting, etc).
MMC	see Microsoft Management Console (MMC)
Mozilla Firefox	A Web browser developed by Mozilla that is ***not*** supported by the DEA E-Commerce program. Firefox should not be used for retrieving CSOS Certificates, however many certificates retrieved using Firefox may still be valid for CSOS ordering.
Netscape Browser	A Web browser developed by Netscape that is supported by the DEA E-Commerce program. Netscape browser is available for download from www.netscape.com.
OID	Object Identifier. Certificate data fields specifically defined by DEA for CSOS certificate information.
Ordering Schedules	See Approved Schedules.
P12 File	A certificate file created by backing up a certificate in a Netscape or Firefox certificate store.
PFX File	A certificate file created by exporting a certificate from an Internet Explorer certificate store.
Private Key	The component of a digital certificate that is kept secret. The private key is used when digitally signing electronic orders and other communications. A digital signature using the private key is proof that the order or communication came from the individual named in the associated certificate.

Private Key Password	A password that protects access to a certificate's secret component used for digital signatures. The private key password is created by the certificate's owner during initial retrieval and when installing the certificate into a certificate store. Any time the certificate is accessed, this password is required, so it is very important not to forget this password. Additionally, DEA has strict requirements for the protection of this password. The password must not be used or known by anyone other than the individual who DEA issued the certificate to.
Public Key	The publicly known component of a digital certificate. The public key is used to verify the validity of digital signatures on electronic orders and other communications.
Relying Party	A participant in an electronic order for controlled substances other than the purchaser. In the majority of CSOS documentation, the term relying party is synonymous with "supplier."
Renewal	The process of requesting a new CSOS digital certificate when the current certificate is about to expire or has already expired. For more information, please reference www.deaecom.gov/renew.html
Retrieval	Synonymous with Activation; The process downloading a CSOS Certificate from the DEA E-Commerce Web site. Technically, this process creates a digital certificate's public and private key pairs, notifies the CA of the public key, and installs the certificate in the client's Web browser.
Revocation	The process of invalidating a digital certificate before it has expired. A revoked certificate is no longer valid for placing electronic orders for controlled substances or for digitally signing communications. For more information, please reference www.deaecom.gov/revoke.html
Root CA	See E-Commerce Root CA
Schedule	See Approved Schedules.
Sub CA	See CSOS Subordinate CA
Subscriber	An individual who has been issued a CSOS digital certificate in his/her name.
Web browser	A software application used for viewing Web pages. Web browsers such as Internet Explorer and Netscape (both recommended) and Mozilla Firefox (not supported by DEA's E-Commerce program) have the capability to retrieve certificates from a Web page and store them in a certificate store.

5. DEA Diversion E-Commerce Support

Please contact DEA Diversion E-Commerce Support for assistance in supporting CSOS subscribers. The support staff has access to customer records and certificate information that may be helpful in troubleshooting customer issues.

Contact Information:

E-mail: csossupport@deaecom.gov

Phone: 1-877-DEA-ECOM
1-877-332-3266

Address: DEA Headquarters
Attention: ODR Mailroom / CSOS
8701 Morrissette Drive
Springfield, VA 22152

The official source for CSOS related information is:

http://www.DEAecom.gov/